



Chief Information Officer
Office of Information Services
Centers for Medicare & Medicaid Services

CMS INFORMATION SECURITY ASSESSMENT PROCEDURE

March 19, 2009

Version 2.0- Final

Summary of Changes in CMS IS Assessment Procedure v2

Significant modifications have been made to the *CMS Information Security Testing Approach*, dated May 13, 2005. Therefore, all sections of this document have been updated and this is a replacement document.

EXECUTIVE SUMMARY

The *Centers for Medicare & Medicaid Services (CMS) Information Security (IS) Assessment Procedure*, hereafter known as “*The Assessment Procedure*” is the CMS-established standard process for all IS assessments. *The Assessment Procedure* provides a common structure for planning and conducting the four (4) assessment phases with consistency throughout the CMS enterprise.

Section 1 - *Introduction*, presents the purpose; core requirements and considerations; goals and objectives. The roles and responsibilities for the assessment process are also elaborated. The roles and responsibilities of the Evaluator, the Facilitator and the Business Owner of the information system to be evaluated, will be distinct and will not overlap or conflict with any other role or responsibility.

Section 2 - *Assessment Planning*, defines the type of assessment; the range of the assessment; the development of assessment plans and scripts; the execution of the assessment; and the exit from the assessment. The Facilitator shall require access to the information contained within the IS Risk Assessment (RA) and System Security Plan (SSP) in order to determine the scope of the assessment effectively. CMS has instituted a three-tiered hierarchical structure in the development of SSPs. At the highest level is the *CMS Master Security Plan*, referred to as the *Master Plan*, which contains all of the enterprise-wide security attributes. An SSP created for a system inherits the attributes of the *Master Plan*; as such, the SSP for an Information System lower in the hierarchy needs only to reference the Master Plan without repeating the details. Similarly, based on the hierarchy depicted in Figure 4, subordinate systems will inherit the controls of the higher system(s)

Assessment Planning includes having clear objectives and constraints for the assessment, a defined budget and assigned resources suitable for the completion of the project, well-defined roles and responsibilities, a structured schedule of defined events and deliverables. The assessment must take into consideration: the type of system; the type of information that is processed, stored or transmitted; the specific type of testing that needs to be performed; the assessment plans that document the major objectives and goals; the test scripts for the execution of the assessment; the evaluation of the controls in place; and the development an assessment report.

Section 3 - *Business Process Analysis*, addresses the comprehensive evaluation of the management, operational and technical security controls implemented to safeguard a CMS information system. It is important to gain a fundamental understanding of the business function(s) supported by the information system. This section provides the Evaluator with guidelines for performing a business process analysis to gain an understanding of the information system. A thorough understanding of the CMS business functions is required for the Evaluator to assess risks and to recommend mitigation strategies for implemented security controls that do not protect the system adequately. To gain an understanding of the business environment, the Facilitator shall provide the Evaluator with the necessary business environment information.

Section 4 - *Document Review*, addresses the analysis of policies, procedures, templates and other relevant documentation related to the information security controls that are under review. The Evaluator shall analyze the security control documentation against the defined assessment objectives to identify discrepancies between IS documentation and implemented controls.

Section 5 - *Interviews*, addresses how the Evaluator shall conduct interviews with key staff members of the system support team to determine how the documented policies and procedures are to be followed. The key point of the interview process is to ensure that the processes conveyed by the interviewee are the same processes that are documented for the information system.

Section 6- *Security Control Assessment*, addresses how the Evaluator shall perform active security testing of the information system to assess the implemented security controls and to identify gaps between the implemented controls and the documented controls. The Evaluator shall capture, document and retain information sufficient to prove the existence or non-existence of vulnerabilities discovered through the assessment process.

Any gaps identified during the documentation review, interviews or security control assessments will be reported in the findings report based on the *CMS Reporting Procedure for Information Security (IS) Assessments*.

TABLE OF CONTENTS

| | |
|--|-----------|
| EXECUTIVE SUMMARY | II |
| 1. INTRODUCTION..... | 1 |
| 1.1. PURPOSE..... | 1 |
| 1.2. OVERVIEW | 1 |
| 1.3. SCOPE..... | 2 |
| 1.4. ROLES & RESPONSIBILITIES..... | 2 |
| 2. ASSESSMENT PLANNING..... | 5 |
| 2.1. OVERVIEW | 5 |
| 2.2. INITIATE | 5 |
| 2.3. PLAN..... | 11 |
| 2.4. EXECUTE | 15 |
| 2.5. MONITOR & CONTROL..... | 16 |
| 2.6. CLOSE..... | 17 |
| 2.7. MITIGATION | 17 |
| 2.8. ADDITIONAL ISSUES | 17 |
| 3. BUSINESS PROCESS ANALYSIS | 18 |
| 3.1. DETERMINE OPERATIONAL STATUS | 18 |
| 3.2. REVIEW PRIOR ASSESSMENT RESULTS | 19 |
| 3.3. REVIEW BUSINESS ENVIRONMENT..... | 19 |
| 3.4. REVIEW SYSTEM ENVIRONMENT..... | 20 |
| 4. DOCUMENT REVIEW | 22 |
| 4.1. ANALYZE DOCUMENTATION | 22 |
| 4.2. IDENTIFY ADDITIONAL DOCUMENTS | 23 |
| 4.3. VALIDATE DOCUMENTED CONTROLS | 23 |
| 4.4. REVIEW PERSONNEL ROLES AND RESPONSIBILITIES | 23 |
| 5. INTERVIEWS..... | 26 |
| 6. SECURITY CONTROL ASSESSMENT | 28 |
| 6.1. IDENTIFY TEST ENVIRONMENT | 28 |
| 6.2. DEFINE ASSESSMENT PROCEDURES..... | 30 |
| 6.3. PERFORM SYSTEM TESTS | 31 |
| 6.4. VALIDATE VULNERABILITIES..... | 35 |
| 6.5. REPORT ASSESSMENT RESULTS | 36 |
| APPENDIX A: ASSESSMENT PLAN INSTRUCTIONS..... | 38 |
| APPENDIX B: TEST SCRIPTS..... | 45 |
| APPENDIX C: RULES OF ENGAGEMENT (ROE) INSTRUCTIONS..... | 49 |

APPENDIX D: COMMON VULNERABILITIES..... 55
APPENDIX E: TESTING TOOLS 58
APPENDIX F: SOCIAL ENGINEERING..... 60
APPENDIX G: RESOURCES & REFERENCES..... 64
APPENDIX H: ACRONYMS..... 65

1. INTRODUCTION

1.1. PURPOSE

An information security (IS) assessment is part of the overall CMS IS program designed to identify IS risks and protect CMS information assets. The *CMS Information Security (IS) Assessment Procedure*, based on guidance provided in The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision A, *Guide for Assessing the Security Controls in Federal Information Systems*, establishes a formal and consistent process for the assessment of CMS information systems and their underlying components to ensure that information assets are secured appropriately. An IS assessment is the process of validating the effective implementation of security controls for an information system based on defined security requirements.

1.2. OVERVIEW

The *CMS IS Assessment Procedure*, hereafter known as “*The Assessment Procedure*”, provides the information system Business Owner, the Evaluator and the Facilitator with a standardized approach for scoping, planning, performing, documenting and managing an information system’s security assessment. Section 1 describes the purpose and scope of the assessment. Section 2 includes the project management framework of the assessment. *The CMS IS Assessment Procedure* further divides the IS assessment process into four (4) aspects as described below and graphically represented in Figure 1: Assessment Phases:

- The *Business Process Analysis*, Section 3, forms the foundation for all subsequent assessment activities. The level and type of technical testing to be conducted shall be dependent upon the information sensitivity, the documented security control requirements and the known business risks.
- The *Document Review*, Section 4, provides for the evaluation of implemented policies and procedures that support the business processes of the information system. Analysis of the documentation provides support for the business process and for the implemented technical controls.
- The *Interview Assessment*, Section 5, provides for interviews with key staff members of the system support team to determine how the documented policies and procedures are to be followed.
- The *Security Control Assessment*, Section 6, provides the Evaluator an opportunity to test and to validate the information system security controls with automated assessment tools and manual efforts.

Figure1: Assessment Phases



While the four (4) aspects are inter-related and inter-dependent, each aspect retains its own distinct goals and objectives that contribute to the overall assessment of the information system.

1.3. SCOPE

The scope applies to IS assessments for all CMS information systems, whether CMS personnel or CMS Data Centers and Business Partners conduct the assessment regardless if they are a General Support System (GSS), a sub-system of a GSS, a Major Application (MA) system, or an application within an MA.

1.4. ROLES & RESPONSIBILITIES

The processes outlined in *The Assessment Procedure* are reliant upon: (i) the capability, competence and constancy of the Evaluator(s) in performing assessment activities; (ii) the cooperation of the Business Owner(s) of the system being evaluated; and (iii) the participation in assessment activities by appropriate CMS personnel.

Table 1: Roles and Responsibilities

| ROLE | RESPONSIBILITIES |
|----------------|---|
| Evaluator | <ul style="list-style-type: none"> • Understand CMS policies, standards, procedures, system architecture and structures. • Limit activities to the assessment scope, but report on all vulnerabilities that may impact the overall security posture of the system. • Refrain from conducting any assessment activities that she/he is not competent to carry out or to perform in a manner which may compromise the information system being assessed. • Develop the <i>Assessment Plan</i> and modify the <i>Test Scripts</i> according to the scope of the assessment. • Prepare a Security Assessment Report (e.g. Findings Report) to communicate how the CMS business mission will be impacted if an identified vulnerability is exploited. |
| Facilitator | <ul style="list-style-type: none"> • Work with CMS IS management to coordinate the planning and execution of the assessment. • Negotiate the development of the <i>Rules of Engagement (RoE)</i> for the assessment. • Review and approve the <i>Assessment Plan</i>. • Review and approve the <i>Test Scripts</i>. • Accept final deliverables. |
| Business Owner | <ul style="list-style-type: none"> • Work with the Facilitator to initiate the assessment project. • Identify the known risks and boundaries of the system being assessed. • Ensure that the system is deployed and operated according to the CMS IS policies and standards. |

| ROLE | RESPONSIBILITIES |
|--|---|
| | <ul style="list-style-type: none"> • Understand how the system is integrated into the CMS information technology architecture. • Update the IS artifacts whenever a significant change occurs. • Maintain an awareness of inherited security controls and their impact upon the system being assessed. |
| CMS IS Management (Chief Information Officer (CIO), Chief Information Security Officer (CISO)) | <ul style="list-style-type: none"> • Develop and maintain IS policies, procedures and control techniques to address system security planning. • Manage the identification, implementation and assessment of common security controls. • Include the evaluation results in the determining the accreditation decision for the information system. |
| Information System Security Officer (ISSO) / System Security Officer (SSO) | <ul style="list-style-type: none"> • Participate in the assessment process by assisting the Facilitator in identifying the appropriate contacts and any relevant support information. • Ensure internal system controls conform to NIST, Department of Health and Human Services (DHHS), and CMS IS policies and standards, and fulfill Certification and Accreditation (C&A) requirements. |

The roles and responsibilities of the Evaluator, Facilitator and the Business Owner of the evaluated information system, will be distinct and will not overlap or conflict with any other role or responsibility.

1.4.1. Evaluator Independence

The NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* states, "If assessment results are to be used for certification activities, then an independent assessment (or independent validation of assessment results) must be conducted". An independent assessment and reporting of vulnerabilities establishes a basis for separation of duties and reduces the risk of potential conflicts of interest. The Security Test & Evaluation (ST&E) as part of the system's Certification and Accreditation (C&A) requires an independent test of all the applicable IS controls, at a minimum, every three (3) years. However, the required annual Security Control Testing (SCT) of approximately one-third of the applicable IS controls does not require independence but is encouraged since independent assessments over a three (3) year period covering all the IS controls can be used to satisfy the system's ST&E requirement. Hence, it is highly recommended that for all IS assessments, the Evaluator is independent from the Organization, the Facilitator and the Business Owner in both attitude and appearance. However, for certain tests, and when resources are limited, the Business Owner can employ staff within the organization as long as there is separation of duties from the information system being assessed.

The Evaluator shall be objective and free of conflicts of interest in discharging his or her professional responsibilities. Evaluators are also responsible for being independent in fact and

appearance when providing assessment services. Objectivity is a state of mind that requires the Evaluator to remain impartial, intellectually honest, and free of conflicts of interest. Independence precludes relationships that may, in fact or appearance, impair objectivity in performing the assessment. The maintenance of objectivity and independence requires continuing assessment of relationships with those involved in the management of the information system. The Evaluator shall exercise due professional care, including observance of applicable professional standards.

1.4.2. Facilitator Independence

In all matters related to the assessment, the Facilitator shall be independent from the Evaluator and the Business Owner, remaining impartial to both as it pertains to the assessment.

The Facilitator is responsible for applying assessment resources efficiently, economically, effectively and legally to achieve the purposes for which the resources were furnished. If the Business Owner contracts out to an independent ST&E Business Partner, the assigned Facilitator must demonstrate a separation of duty from areas under review. In the event that the Business Owner contracts an independent ST&E consultant, the assigned Facilitator must demonstrate a separation of duty from areas under review and no direct supervisory influence by the Business Owner.

2. ASSESSMENT PLANNING

2.1. OVERVIEW

The Assessment Procedure provides a standardized approach for the planning of an IS assessment for a CMS information system and its underlying components. The Business Owner is responsible for ensuring that each security assessment has:

- A budget and assigned resources suitable for the completion of the project
- Clear objectives and constraints
- Well-defined roles and responsibilities
- Specific starting and ending dates within a structured schedule of defined events and deliverables

This Assessment Planning section provides a guideline for the successful completion of an assessment following the project management framework in Figure 2.

2.2. INITIATE

The assessment process begins when a Business Owner determines that a security assessment is required for an information system.

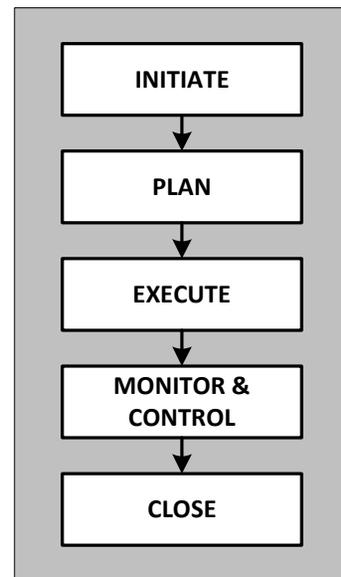
The Business Owner must develop a scope statement that is dependent upon, but not limited to, the following factors:

- (1) Overall system security level of the system;
- (2) Known business risks associated with the information system;
- (3) System Boundaries;
- (4) Dependence of the system upon the hierarchical structure;
- (5) System development phase;
- (6) Documented security control requirements;
- (7) Assessment type;
- (8) Assessment range;
- (9) Assessment objectives; and
- (10) Budget considerations.

The scope will also identify the stakeholders and document any additional expectations of the Business Owner.

The Facilitator shall require access to the information contained within the IS Risk Assessment (RA) and System Security Plan (SSP) in order to determine the scope of the assessment effectively. Based on the Facilitator's review, the assessment scope will need to be negotiated

Figure 2: Project Management Framework



with the Business Owner. The Facilitator shall then alert other security officers, management, and users that an assessment is taking place.

The initiation of a new assessment within CMS follows a process where the first consideration must be the federal mandates that govern the type of system involved. Depending upon the system and the type of information that is processed, stored or transmitted, certain standards must be followed and certain methodologies must be employed. If the testing is being done for the first time, or is being outsourced to a third party with no known experience in this type of testing for the organization, then the appropriate contracting vehicle for testing must be determined.

The next step in the assessment initiation process is for the Business Owner to determine that specific testing needs to be performed. This might be dictated by legal or contractual requirements; however, the Business Owner drives the decision.

Once the appropriate standards and methodologies are known and the Business Owner determines that testing needs to be done, the precise information system to be tested must be identified. This includes all information stored, processed or transmitted, all hardware resources that comprise the system (computers, networking infrastructure, etc), all software resources that comprise the system, and finally, all of the personnel that maintain and run the system.

The contracting vehicle is determined taking into consideration, the evaluator selected and the experience of the evaluator in performing testing for the organization.

Once the contract vehicle is determined, the Business Owner must be reconfirmed based on the contract vehicle selected. The Business Owner will then identify any additional points of contact related to the system. This usually breaks down along functional lines. For example, in a system relying upon a publicly facing web application with a back-end database, the Business Owner may identify points of contact relevant to systems, networking, database administration, web administrators or others as applicable.

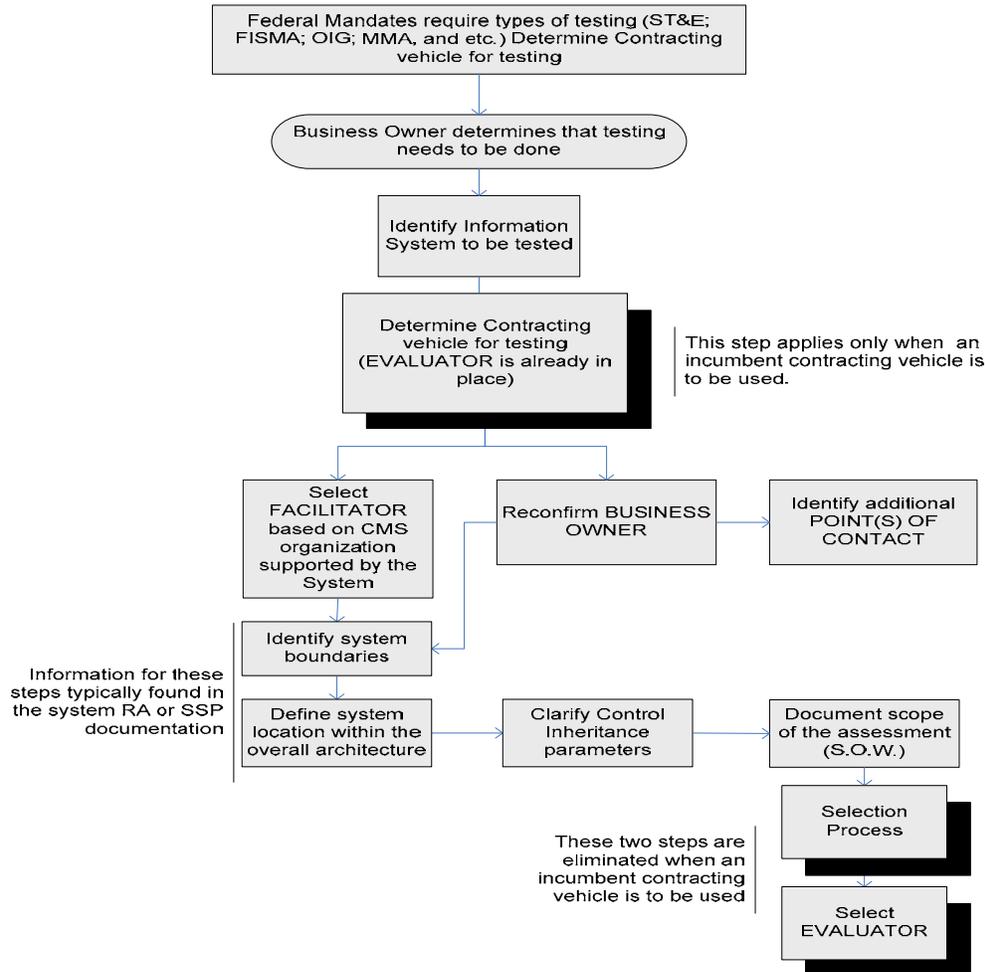
Parallel to the confirmation of the Business Owner is the selection of the CMS Facilitator. This will be dependent on the system to be tested. The CMS Facilitator will ensure that testing is completed thoroughly and efficiently.

With the Business Owner and the CMS Facilitator identified, the next step is to refer to the Information Security (IS) Risk Assessment (RA) and System Security Plan (SSP) to: 1) identify the boundaries of the system to be tested; and 2) define the system's location within the overall architecture of the organization. Having these two (2) activities clearly defined guards against performing testing out of scope.

The clarification of control inheritance parameters are required to complete a Scope of Work for the assessment. In addition to defining the system boundaries and locating the system within the overall architecture, an understanding of all relevant controls and how they are inherited throughout the system is required to evaluate their effectiveness in protecting the confidentiality, integrity and availability (CIA) of the system's data.

With the Scope of Work completed, selection of a vendor for testing (if one does not already exist) may now proceed. See Figure 3 Below for the Assessment Initiation Process Flow.

Figure 3: Assessment Initiation Process Flow



The Evaluator selection process may be omitted if CMS IS Management has previously determined the Evaluator based on an on-going contractual relationship in accordance with the Office of Acquisition and Grants Management (OAGM) approved contracts.

2.2.1. Overall system security level of the system

The Business Owner shall have identified the overall system security level of the system being assessed in accordance with the *CMS Systems Security Level by Information Type*, as documented in the IS RA and SSP. The assessment shall be commensurate with that system security level. A system with a HIGH system security level will require a higher level of

scrutiny since deficiencies in such a system will present a significantly greater risk to CMS than a system with a LOW system security level.

2.2.2. Known business risks associated with the information system

The Business Owner shall provide the Evaluator the IS RA that identifies any known deficiencies in the information system within the scope statement to ensure that the Evaluator is able to focus on these specific items. Likewise, the Evaluator shall identify any suspected deficiencies in the information system based on the system information provided.

Example: A Business Owner knows that the web-based application does not use hypertext transfer protocol (HTTP). The Evaluator may then suspect, based on his/her knowledge of web applications, that the underlying middleware identified in the SSP may expose the overall enterprise to several vulnerabilities. Both issues shall be included in the scope to ensure that specific data security and application vulnerabilities related to the web application are reviewed during the assessment.

2.2.3. System Boundaries

The Facilitator, the Business Owner and the Evaluator shall have a clear understanding of what constitutes the boundaries of the system to be assessed, including any applicable interfaces with other systems. This includes physical, logical and virtual boundaries around a set of processes, communications, storage devices and related resources. The Evaluator will verify and validate these boundaries as part of the review of the SSP, the interview process and the penetration test.

The Evaluator must be mindful that CMS utilizes a Federal Information Security Management Act (FISMA) “*Application Family*” concept in describing MAs. A *Major Application Family* consists of multiple applications that support the same business function and the family is managed under a single CMS Center or Office. Assessments are conducted routinely on an individual application within the *Major Application Family*, not the entire family.

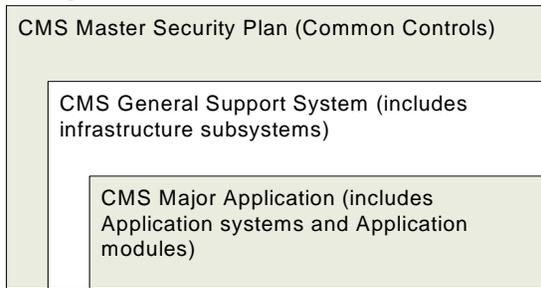
2.2.4. Dependence of the System upon Hierarchical Structures

CMS has instituted a three-tiered hierarchical structure in the development of SSPs. At the highest level is the *CMS Master Security Plan*, referred to as the “*Master Plan*”, which contains all of the enterprise-wide security attributes. These also are known as “Common Controls”. An SSP created for a CMS system inherits the attributes of the *Master Plan*. As such, the SSP for an information system lower in the hierarchy needs only reference the *Master Plan* without repeating the details. These controls may not be fully documented in the *Master Plan* but will exist in other Agency documentation. If the information system applies controls that are different from those defined in the Master Plan, these controls are to be defined in the respective information system SSP. Figure 4, below, depicts the various levels in the overall CMS security control hierarchy.

The next tier is the GSS including all related infrastructure subsystems. Infrastructure level assessment is an examination of the GSS that supports MA(s) that operate within the GSS environment. This may include a review of all supporting devices, including networking

equipment, telecommunications equipment, servers, desktop and workstations that are generally not dedicated to any single MA.

Figure 4: CMS Inheritance Hierarchical Structure



Application level assessment is a review of the MA and related application systems or of an individual application system. This includes a review of all links to other interconnected or inter-related systems, as well as direct attempts to subvert the implemented security controls of the application.

This hierarchical structure also exists for information systems that support CMS but exist outside of the CMS enclave. This can include an external Medicare Processing Data Center or a site that hosts a CMS application from an external location. The Facilitator must consider the location of the information system, as well as the location of the system within the hierarchical structure of the host environment.

2.2.5. CMS Integrated IT Investment & System Life Cycle Framework Phase

The Facilitator and the Business Owner shall determine what phase of the CMS Integrated IT Investment & System Life Cycle Framework (“Framework”) applies to the information system. The Facilitator must be cognizant that an assessment performed on an information system in a test or development environment might only apply to that environment unless the Business Owner can clearly demonstrate that the test or development environment suitably replicates the production environment on which the information system is expected to operate.

2.2.6. Assessment Type

Various types of IS assessments are required within CMS. These may include, but are not limited to, the following:

- **Security Test & Evaluation (ST&E)**
The ST&E is a third-party process conducted by an independent Evaluator to assess the management, operational and technical controls of a specified information system. The ST&E includes the execution of assessment procedures and techniques designed to evaluate the effectiveness of security controls in a particular environment, and to identify vulnerabilities in an information system after the implementation of safeguards. An ST&E is required for initial C&A and every three (3) years thereafter. The exception to this is when there is a major change, a change in the security environment or a major security violation.
- **Annual FISMA Security Control Assessment (FA)**
All information systems used or operated by an agency or by a business partner of an agency or other organization on behalf of an agency must be assessed at least every 365

days. These may be performed internally by the agency. FISMA (section 3544(b) (5)) requires “periodic testing and evaluation of the effectiveness of IS policies, procedures and practices, to be performed with a frequency depending on risk, but no less than annually.”

FISMA does not require the annual assessment to include all security controls employed in an organizational information system. However, all security controls must be assessed over a three (3) year period. The Business Owner shall test approximately one-third of the security controls in any given annual assessment. If annual testing is performed by an independent Evaluator, and over a three (3) year period covering all internal controls, the results of the annual assessment may be utilized to comply with the ST&E requirement.

- Other vulnerability assessments as required
There are several other types of security assessments designed to assess the susceptibility of a particular system to specific types of attacks. These include, but are not limited to, the following:
 - Network Scanning
 - Vulnerability Scanning
 - Password Cracking
 - Log Review
 - Integrity Checkers
 - Virus Detection
 - War Dialing / Driving
 - Penetration Testing

The Facilitator shall work with CMS Management and the Business Owner to determine what type of assessment is required to meet CMS requirements.

Other audits, assessments and evaluations may be required including, but not limited to the Medicare Modernization Act (MMA); Section 912 evaluations; A-123 reviews, and Chief Financial Officers (CFO) audits. These may follow independent assessment methodologies and may not conform to *The Assessment Procedure*. The results of these additional assessments, however, shall be provided to the Evaluator by the Business Owner, the Facilitator or by CMS Management as required for possible use in meeting the FISMA testing requirements. If the assessment occurred within the last 365 days; adequately tested the controls in compliance with NIST SP 800-53A; and met the requirement for independence, NIST has allowed each agency to use such assessment results for FISMA compliance.

2.2.7. Assessment Range

An assessment can be defined as anything from a limited test of certain controls for a specific system component to a comprehensive evaluation of an entire system. If the assessment scope is comprehensive, the Evaluator shall be expected to evaluate all security elements, including those that are inherited. Where it is clearly understood that a system inherits controls from the hierarchy, the Facilitator and Business Owner shall clearly identify, in the assessment scope, the inherited controls and the Evaluator limitations for testing inherited controls.

2.2.8. Documented Security Control Requirements

The CMS IS Program has incorporated the requirements for FISMA, the Health Insurance Portability and Accountability Act (HIPAA), Internal Revenue Service (IRS), Federal Information System Controls Audit Manual (FISCAM) and various Office of Management and Budget (OMB) circulars and memorandums in its policy and standards as defined at <https://www.cms.hhs.gov/informationsecurity>. CMS has developed *CMS Information Security Test Scripts* with Assessment Criteria and Assessment Objectives based on NIST SP 800-53A for all these controls. Similarly, these same criteria and objectives are included in the CMS Minimum Security Requirements (CMSR). The Facilitator shall identify security control requirements from these test scripts to meet the scope of the assessment.

2.2.9. Assessment Objective

Assessment objectives are defined in the test scripts and in compliance with NIST SP 800-53A. CMS Management may assign other assessment objectives, as needed, to support the CMS IS Program.

2.3. PLAN

Assessment planning is critical to the allocation of resources and achieving an understanding of what activities will occur during the assessment, and should be part of an overall information system project management plan.

2.3.1. Develop Assessment Plan

The Evaluator shall prepare assessment plan that documents the major objectives and goals for the assessment. The assessment plan shall include the use of the CMS provided test scripts as described in Appendix B. The Evaluator shall utilize the test scripts as provided and only modify the scripts within the scope of the assessment. The Evaluator shall map out the execution of the test scripts that shall include the following assessment methods and appropriate procedures as defined in the test scripts to validate the effectiveness of the documented and implemented safeguards:

- Interview: Focused discussions with individuals or groups to facilitate understanding, achieve clarification, or obtain evidence.
- Examine: Checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
- Test: Exercising one or more assessment objects under specific conditions to compare actual with expected behavior.

The Evaluator shall also include procedures in the assessment plan for the review of corrective actions developed for past findings that remain open. The Facilitator shall provide a list of open findings, as reported in the CMS Integrated Security Suite (CISS), to the Evaluator to ensure that the evaluation of past findings is completed concurrent with new assessment activities.

The Evaluator shall submit the draft assessment plan to the Facilitator. The Facilitator and Business Owner shall have an opportunity to review and to comment on the assessment plan and

request that the Evaluator make necessary adjustments before assessment procedures begin. Assessment procedures may not begin until the Facilitator approves the assessment plan.

Appendix A provides instructions and a template for the development of an *Information Security Assessment Plan*.

2.3.2. Determine Common Security Controls and Control Inheritance

Any information system may inherit the implementation of a security control from associated information systems, the IT infrastructure, other GSSs, or from agency-wide policies and procedures. In order to minimize the duplication of testing efforts, the Evaluator shall analyze the business processes supported by the information system to understand what security controls, if any, are inherited from other sources. It is expected that the Business Owner, as part of the IS RA and SSP documentation, will have already identified and documented the controls that are inherited.

The Facilitator and the Evaluator shall then determine which portions of the inherited security control families need to be re-tested to assess whether there are any residual risks or to validate documented statements regarding control inheritance based on the risk level of the information system and the currency of the testing of the inherited controls.

2.3.3. Leverage Prior Assessment Data

To improve the overall assessment process, the Business Owner shall be aware of, and have records for, any prior assessment of the information system. The Evaluator, to the extent possible and in accordance with the *Rules of Engagement* (RoE), shall make use of all security documentation and prior assessment information maintained by the Business Owner. Evaluators shall be expected to review prior assessment data with an understanding of CMS business processes.

2.3.4. Modifying Test Script

The Facilitator shall provide the Evaluator with CMS test scripts to serve as a baseline for the objectives applicable to the assessment. The Evaluator shall further enhance the test scripts to support the assessment plan by providing detailed criteria to be used in validating the implementation and effectiveness of documented security controls.

The security assessment is expected to go beyond simple checklists and pass/fail results to evaluate the effectiveness of implemented security controls. The test script, following the current issuance of NIST SP 800-53A, shall include guidance for technical testing and/or verification and the review of device configuration, as well as questions pertinent to the interview of information system personnel and key analysis points that apply to the documentation review.

- The Evaluator shall include standard interview questions in the script document to assist in determining whether vulnerabilities exist.

The Evaluator shall submit the draft test scripts to the Facilitator. The Facilitator, Business Owner and CMS Management shall have an opportunity to review and to comment on the test scripts and request that the Evaluator add or remove items from the test script before the assessment begins.

2.3.5. Assign Staffing Resources

If an independent assessment is conducted, the Evaluator shall assign only skilled, experienced and objective individuals to conduct the assessment. Security assessors should have significant skills and experience with the assessment method and techniques identified for the engagement. Assigned staff shall be available for all aspects of the assessment, including assessment preparation, data analysis and report development.

The Evaluator shall provide the resumes of personnel intended to conduct the assessment for the purpose of approval by the Facilitator and/or the Project Officer. The Project Officer and/or Facilitator shall review the resumes for relevance, according to the staff requirements documented within the Assessment Contract.

All Evaluator's personnel who shall participate in the assessment process must submit to the requisite clearance procedures for Public Trust Level 5 Moderate Risk or Level 6 High Risk positions, as specified in the HHS Personnel Security/Suitability Handbook. The Office of Operations Management (OOM) and Security and Emergency Group (SEMG) may grant approval of personnel to conduct the assessment, upon completion and positive results from fingerprinting.

For every assessment, the Evaluator, the Facilitator and the Business Owner, shall review any relationships between the Evaluator and the system being assessed to establish the independence of the Evaluator. If an individual recruited to perform security assessment is involved with the development, maintenance or administration of the system being assessed, the Business Owner and the Facilitator shall review the relationship between the Evaluator and the system to ensure that sufficient separation of duties exists between the system administrators and the security assessment team. For example, some business partners, e.g., "small businesses" or internal components have limited resources to conduct an assessment. However, should they conduct the assessment that does not use external independent business partners, an attestation / demonstration of sufficient separation of duties needs to be provided.

2.3.6. Define Assessment Schedule

The Facilitator, the Business Owner and the Evaluator, shall establish and maintain a schedule for the assessment to ensure that a suitable amount of time is provided to complete test activities. The baseline schedule, current schedule and all subsidiary schedules shall contain project deliverables, activities and milestones. See Table 2 below for a suggested baseline schedule.

Table 2: Baseline ST&E Schedule

| ASSESSMENT PHASE | ASSESSMENT ACTIVITY | ROLE | TIMING (Relative to Assessment) |
|-------------------------|--|--|--|
| INITIATION | Determine type and scope of assessment | Facilitator CMS Management | 8+ weeks prior |
| PLANNING | Deliver notification to Business Owner | Facilitator | 8 weeks prior |
| | Evaluate and finalize scope | Facilitator Evaluator Business Owner | 7 weeks prior |
| | Deliver Rules of Engagement and Documentation Request | Evaluator | 6 weeks prior |
| | Introductory Call | Evaluator Facilitator Business Owner | 6 weeks prior |
| | Delivery of Key Documents | Business Owner Facilitator | 5 weeks prior |
| | Deliver Draft Assessment Plan | Evaluator | 4 weeks prior |
| | Draft Assessment Plan Meeting | Evaluator Facilitator Business Owner | 3 weeks prior |
| | Deliver Final Assessment Plan | Evaluator | 2 weeks prior |
| | Deliver additional system, policy and procedure documentation relevant to the test scope | Business Owner | 2 weeks prior |
| EXECUTION | Assessment Preparation | Evaluator | 1 – 2 weeks prior |
| | Assessment Activities (on-site or remote) | Evaluator Business Owner | Typically 1 week on-site or remote |
| | Assessment Analysis and Findings Development | Evaluator | 1 – 2 weeks after |
| | Delivery of Draft Report | Evaluator | 3 weeks after |
| | Draft Report Meeting | Evaluator Facilitator Business Owner | 4 weeks after |
| | Complete Final Report | Evaluator | 5 weeks after |
| CLOSE | Final Package | Evaluator | 5 weeks after |
| | Complete Book | Evaluator | 6 weeks after |

This schedule is an example and may not be suitable for all assessments. The Facilitator, Evaluator and Business Owner shall determine an appropriate schedule based on the assessment scope, budget constraints and resource limitations.

2.3.7. Establish Rules of Engagement (RoE)

The RoE is the governing document established for the assessment through negotiation between the Facilitator and Evaluator. The Evaluator shall provide the Facilitator with a RoE document that defines the scope of the assessment; the assessment period; the type of assessment that will be performed; management requirements; resource requirements; and the handling of the output resulting from the assessment.

Appendix C provides instructions for the development of a *CMS IS Assessment Rules of Engagement* document.

2.3.8. Provide Documentation Request

The Evaluator shall prepare a list of documents that may be needed to complete the assessment. The list shall be provided to the Business Owner through the Facilitator and the requested documents shall be provided to the Evaluator. The transmittal of ALL sensitive information shall be in accordance with CMS IS policy. The Business Owner shall furnish all available requested documentation to the Facilitator in a timely fashion to avoid unnecessary cost overruns.

As the Facilitator receives the requested documents from the Business Owner, the Facilitator shall then provide the received documents to the Evaluator in a timely fashion. The Facilitator shall also inform the Evaluator regarding any missing or unavailable documentation.

At all steps in the request process, records shall be maintained by the Facilitator to track requests made, requests fulfilled and outstanding requests. The Evaluator should furnish any documentation requests prior to the start of the assessment procedures; however, requests for documentation may be made at any point during the overall assessment project.

2.4. EXECUTE

2.4.1. Documentation Review

The Facilitator shall receive a request for documents that are to be delivered to the Evaluator within a pre-determined time frame for review prior to the start of the assessment. All other documents shall be delivered in a timely manner to maximize efficiency while conducting the assessment. The cooperation of the Business Owner and the support personnel for the information system being evaluated is critical to the success of the assessment.

2.4.2. Evaluate Recent Security Assessment Documentation

The Evaluator shall assess the usefulness and appropriateness of prior reports and should consider any significant findings reported by the other auditors or experts. The Evaluator shall use independent professional judgment to determine the suitability of prior assessments and recommend to the Facilitator whether a re-assessment is required. Ensuring compliance with mandates and requirements, the Business Owner and the Facilitator shall make the final decision as to whether re-testing is required.

2.4.3. Evaluate Corrective Action Plans (CAPs)

The Evaluator shall validate the effectiveness of completed corrective actions to close or reduce the impact of all vulnerabilities discovered during prior assessments, and to re-test open vulnerabilities not corrected. The following suggested sources of information shall be reviewed for validation of the closure or reduction:

- ST&E reports
- Annual FA
- Audit reports
- Vulnerability assessment / penetration test reports

2.4.4. Technical Testing

The Evaluator shall follow a documented methodology for technical testing to ensure that the results can be reproduced by the Business Owner or the technical support staff; can be verified by a third party; and can be validated by CMS Management for use in other assessment activities. Section 6 provides procedures for the execution of technical testing.

2.4.5. Security Control Analysis

The Evaluator shall follow the pre-defined assessment plan and test scripts to assess the implemented security controls and identify threats, related vulnerabilities, and the residual risk to the information system. After reviewing the threats and vulnerabilities for completeness, the Evaluator shall analyze the selected security controls to ensure that the risk mitigation strategy is appropriate for minimizing the risk to CMS' ability to conduct business.

2.5. MONITOR & CONTROL

Progress reviews on the assessment shall occur as a forum for the Evaluator, the Facilitator, the Business Owner and CMS Management to discuss the assessment status. During the assessment period, additional status checks may be required to ensure that the Evaluator informs all stakeholders of the assessment progress and advises the Facilitator of any issues encountered so that they can be resolved before the assessment is concluded. At a minimum, the following status activities will be held:

- Assessment Plan Review
- Entrance conference (call)
- Exit conference (call)
- Draft Report Review Meeting

Daily status calls are optional, depending upon the complexity of the environment or as the Business Owner requires.

2.6. CLOSE

The Evaluator shall develop an assessment report following the *CMS Reporting Procedure for IS Assessments*, based on the current reporting procedure. A draft of the report will be provided to the Facilitator for review within ten (10) business days following completion of technical testing. The Facilitator shall ensure that the draft report successfully meets the scope and objectives for the assessment. Within ten (10) business days following the receipt of the report from the Evaluator, the Facilitator shall schedule a meeting between the Facilitator, the Evaluator and the Business Owner to discuss the findings. Remediation of any discrepancies shall occur within five (5) business days following the meeting. The Evaluator shall finalize and submit the report to the Business Owner through the Facilitator within five (5) business days following the remediation period.

2.7. MITIGATION

The Business Owner shall provide the CAPs to the Enterprise Architecture and Strategy Group (EASG) following the *CMS Plan of Action & Milestones (POA&M) Guidelines* for each open finding identified in the final report. A POA&M must be created for every weakness that requires remediation.

2.8. ADDITIONAL ISSUES

2.8.1. Non-Disclosure Agreement (NDA) / Adjudication

Access to government information shall be granted upon demonstration of a valid need to know, and not be based merely upon position, title, level of investigation, or position sensitivity level. NDAs are to be signed prior to access by anyone who requires such access to government and/or sensitive information.

2.8.2. Follow-Up

Following the assessment, the Business Owner, the Evaluator or the Facilitator may review the assessment process to develop feedback on the successes or failures of the process. This follow-up review is optional and at the discretion of those involved in the assessment. Information collected in this way may be submitted to EASG to support the on-going evaluation of the assessment processes of the CMS IS Program.

2.8.3. Post-Assessment Support

The Evaluator shall provide support after the assessment to clarify findings, to review proposed CAPs, and to validate corrective actions to ensure that the remediation addresses the risks described in the findings.

3. BUSINESS PROCESS ANALYSIS

In order to conduct a comprehensive evaluation of the management, operational and technical security controls implemented to safeguard a CMS information system, it is important to gain a fundamental understanding of the business function(s) supported by the information system. The following sections provide the Evaluator with guidelines for performing a business process analysis to gain an understanding of the information system.

3.1. DETERMINE OPERATIONAL STATUS

The Evaluator shall determine the operational status of the information system under review. This status can be operational, under development, or undergoing a major modification, as defined below.

Table 3: System Operational Status

| Status | Definition | Assessment Requirements |
|-------------------------------|---|---|
| Operational | The system is currently in production and supporting a business function. | The SSP, the IS RA and the supporting documentation will drive the system assessment requirements. |
| Under Development | The target system is in the “Design and Engineering”, “Development”, “Testing”, or “Implementation” phase of the CMS Framework. | Identify the current phase in order to determine suitable assessment requirements. Assessment may be performed in any phase of the CMS Framework to evaluate the effectiveness of the developed security controls prior to being moved to production. |
| Undergoing Major Modification | The system to be assessed is in the process of a major transition or conversion. | Review the processes followed to ensure that security is being considered during each phase of the design of the modification. Evaluate the design documentation for the modification to establish that security controls are appropriately developed, tested and implemented. Verify that the system documentation has been evaluated and updated appropriately to address the system changes. |

3.2. REVIEW PRIOR ASSESSMENT RESULTS

The Facilitator shall provide copies of open findings, audits, reviews or studies that have been conducted within the last 365 days. These include, but are not limited to:

- Government Accountability Office (GAO) reports;
- Office of Inspector General (OIG) reports;
- Internal audit reports;
- Internal reviews;
- FA reports;
- Reports of Congressional hearings; and
- Copies of Congressional testimony.

3.3. REVIEW BUSINESS ENVIRONMENT

A thorough understanding of CMS' business functions is required in order for the Evaluator to assess risks and to recommend mitigation strategies for implemented security controls that do not protect the system adequately. To gain an understanding of the business environment, the Facilitator shall provide the Evaluator with the business environment information including, but not limited to, the following:

- Mission statement for the Information System;
- General description of the Information System business function(s); and
- Interdependencies between the Information System under review and any other CMS business functions.

The Evaluator shall also request copies of brochures, booklets, pamphlets, etc., that document or are related to the business function, automated applications or operations. In addition, the Evaluator may request, from the Facilitator, any overview diagram(s) that document the business function data flow. This should cover the major inputs and data entry points, data flows, communication networks, process sites and major outputs and output points.

From the information provided, the Evaluator shall be able to identify and document all assets related to the assessment, including information types and personnel supporting the business function. Subsequent assessment activities, including the review and identification of business and technical risks, will be based on the sensitivity and criticality requirements of the business function.

3.3.1. Criticality of Business Function

The criticality of the business function is largely a measure of the reliance that CMS or the public places upon the continued CIA of the function.

CMS has established categorizations, based on Federal Information Processing Standards (FIPS) 199 categorization the *CMS System Security Levels by Information Type*, that define the criticality of the information system requirements as Low, Moderate or High. These categorizations determine the level of security controls required to be implemented as part of the

information system. In turn, this affects development of the application assessment plan and the selection of the appropriate test scripts to validate the effectiveness of such controls.

3.3.2. Business Portability

In addition to evaluating controls and procedures, it is necessary to identify any business portability implications. The portability implications are determined by the business function's requirements, which could be driven by the need to distribute software, developed and tested at CMS, to CMS business partners off-site. Alternatively, an application could be hosted at a non-CMS site, or a change of host-site might be required. Any business portability implications identified must be addressed during the system environment review.

The Evaluator shall note any technical portability requirements that the assessment plan should address. During the execution of the assessment procedures, the Evaluator shall identify portability shortfalls as a "finding" in the security assessment report.

3.4. REVIEW SYSTEM ENVIRONMENT

In order to understand the system environment, the Evaluator shall obtain a general description of the technical specifications of the business function by interviewing the appropriate personnel and by requesting copies of relevant documentation. Refer to the test scripts described in Appendix B for applicable documentation for each control. This review will include any environmental or technical issues that may raise special security concerns such as dial-up access, system interconnections, e-authentication and/or portability requirements.

The Facilitator shall provide the Evaluator with an inventory of the hardware, software, network connections and any other relevant technical information associated with the information system. The relationship between system-specific components and any GSS dependencies shall be identified. The Evaluator may also need to request information from the GSS SSP in order to evaluate the relationship between the system being assessed and the GSS environment.

When assessing a larger, shared GSS and in cases where applications have dedicated GSS resources and are not reliant upon a shared GSS environment, the Evaluator shall review the inventory list provided and validate, at a minimum, that the following components are accounted for in the system or GSS documentation:

- System specifications and the operating system (OS), e.g., Windows, AIX, Solaris, Novell, MVS, z/OS;
- Database management systems, e.g., DB2, IMS, IDMS, ADATABASE, ORACLE, DATACOM, Structured Query Language (SQL) Server;
- Peripherals and their technical specifications, e.g., location and the quantity of master consoles, direct access storage devices, other storage devices, optical scanners, modems, tape units, disk units, printers, communication controllers (by type), intelligent terminals (and purpose), dumb terminals;
- Network infrastructure components, related directly to application technical environment, e.g., firewall, router, switch, hub;

- The telecommunications environment including any cooperative processing; any agreements negotiated between the parties such as the Interconnection Security Agreement (ISA), or a Data Use Agreement (DUA); use of Electronic Data Interchange (EDI); use of e-authentication; authentication controls; and any system interconnections or information sharing, along with system identifiers;
- Tape management systems;
- Program library software for source code;
- Program library software for object code;
- Job accounting software;
- On-line program development system software;
- Access control software;
- Audit software packages;
- Report writer / generator software;
- Network master control system software;
- Job entry subsystems;
- Job scheduling systems;
- Performance monitoring software;
- Dial-up security software packages; and
- Technical portability requirements.

Using the list above as a guide to the types of possible infrastructure components, the Evaluator shall compile a detailed list of system components supporting the environment of the information system. The compiled list shall be compared to any diagrams obtained by the Facilitator that describe the relationships between: information systems; major peripherals; network(s); network topology; speed and type of communication links; and the use of modems and terminals.

As part of the system environment review, the Business Owner shall provide any available processing statistics and abnormal termination (“abend”) data. The Evaluator may use the provided statistics to identify operational problems such as excessive downtime, system utilization, or storage capacity issues. System processing statistics include: a breakdown of the most recent system usage and availability by quantifying Central Processing Unit (CPU) (or other processing unit) production processing; test processing; re-run processing; maintenance efforts; idle time; unplanned downtime; and any other available processing statistics. Abnormal terminations statistics shall be broken down by type: systems software; application software; hardware; operator error; or any other category for which data are available.

4. DOCUMENT REVIEW

The Evaluator shall perform a review of all IS documentation related to the scope of the assessment. The Evaluator shall identify and document, at a minimum, any of the following conditions as a finding in the assessment report:

- 1) Undocumented security controls;
- 2) Incomplete documentation for existing security controls;
- 3) Discrepancies between the documented controls and CMS security requirements;
- 4) Gaps between the security control documentation and the required safeguards; and
- 5) Inadequate controls for the recommended safeguards.

4.1. ANALYZE DOCUMENTATION

The Evaluator shall analyze the security control documentation against the defined assessment objectives in the test scripts to identify discrepancies between IS documentation and implemented controls. For example, the SSP controls may be inconsistent with CMS organization requirements, or the components list in the SSP may not be consistent with the system diagram or architecture documentation.

4.1.1. Developmental, Draft and Final Releases

Documents which are identified as “Draft,” or are otherwise incomplete, are not suitable for assessment purposes. The intent of the Document Review is to evaluate final releases of documentation to demonstrate that security controls are implemented in a production system. The only exceptions are the SSP and the IS RA which are not in final versions until after an ST&E has been conducted. In such cases, the previous Corrective Action Plan (CAP) Worksheet and the CAP Review Worksheet will determine what courses of action have been taken and are planned for risk mitigation.

4.1.2. Templates

Some system documents are expected to follow a published CMS standard template. Such templates are developed to ensure that the system specific document meets defined regulations, standards or guidelines. Deviations from established templates may constitute a weakness as they may expose CMS to additional risks or indicate a failure to address key requirements. CMS standard templates are located at: (<http://www.cms.hhs.gov/InformationSecurity>). The Evaluator shall compare the final document to the published templates. However, based on when the documentation was developed, previous versions of the template may be “grandfathered” until the next update is required.

4.1.3. Policy Evaluation Guidelines

The Evaluator shall evaluate information security policies within the context of the CMS IS Program. In accordance with Section 2.2.4, an information system may inherit policy within the CMS hierarchical structure, including another GSS, an MA higher in the hierarchy, or from the

CMS Master Plan as an Agency. The Facilitator shall assist the Evaluator in determining the policy boundaries.

4.1.4. Procedure Evaluation Guidelines

CMS has implemented standardized procedures for developing specific IS documentation in compliance with NIST and DHHS requirements. The Business Owners are subject to these procedures when developing their security documentation, (e.g. SSP, IS RA, etc.).

4.2. IDENTIFY ADDITIONAL DOCUMENTS

The Evaluator shall review all security control documentation appropriate to the scope of the assessment. In addition to the IS RA, the SSP and business process documentation provided according to section 3, the Evaluator shall identify, and request from the Facilitator, additional documentation containing security controls descriptions and requirements, including, but not limited to, the following:

- Technical design documentation;
- Network, system and application diagrams;
- System Logs and Rule sets;
- Configuration documentation, including baseline and as-installed information;
- e-Authentication documentation;
- Memoranda of Understanding / Interconnection Security Agreements; and
- System architecture documentation.

4.3. VALIDATE DOCUMENTED CONTROLS

The Evaluator shall review the provided documentation to validate that the required documentation exists; that it meets the criteria identified in the test scripts; and that it is comprehensive and accurate in its depiction of how the implemented controls provide the necessary safeguards. The Evaluator shall be expected to utilize test scripts for the assessment, as identified in Sections 2.2.8 and 2.3.4 that will include detailed criteria to measure actual implementation and effectiveness of documented security controls.

4.4. REVIEW PERSONNEL ROLES AND RESPONSIBILITIES

The responsibility for securing a CMS information system ultimately rests with the Business Owner. All system users may affect system security, whether the user is a CMS employee or a supporting Business Partner. As such, all users of CMS information systems are obligated to contribute to the maintenance of the CIA of that system.

4.4.1. Key Personnel

After collecting and reviewing all relevant system and/or application documentation, the Facilitator shall conduct an introductory meeting with the Evaluator and the Business Owner to review the scope of the assessment engagement and the logical and organizational boundaries of

the system and/or application. Other attendees of this meeting may include Business Partners and CMS personnel responsible for: 1) managing the business function, and 2) the IS for technical support of the information system.

The attendees identified above shall be present to gain an understanding of the purpose, methodology and scope of the review and the subsequent assessment to be developed. They should also be available to give perspective on any issues encountered during the previous stages of this review and identify the responsible and most qualified individual(s) to answer any questions.

During this meeting, the Evaluator and CMS shall determine the requirements, and potential candidates, for interviews with CMS or Business Partner personnel during the review. For any identified candidates, the Facilitator shall schedule the appropriate meetings. Personnel to be interviewed shall be identified by their functional responsibilities for the information system being assessed, not by their organizational job title.

4.4.2. Relevant Roles and Responsibilities Documentation

The Evaluator shall review the available documentation for the following security-related personnel security controls. While they apply to all roles, the level of the control will vary according to the level of responsibility and the exact nature of the position. The Evaluator shall consider the following when reviewing the roles and responsibilities documentation:

- References are verified and background checks conducted when evaluating prospective employees;
- Periodic re-investigations are conducted on employees;
- When granted access to sensitive information, employees and Business Partners are required to sign confidentiality and security agreements;
- Employees are required regularly to schedule vacations that exceed several days while their work is temporarily re-assigned;
- Termination and transfer procedures include: exit interviews; return of CMS property, keys, identification cards, passes, etc.; notification to security management and prompt revocation of system access; confirming the length of non-disclosure requirements and under certain circumstances, escorting terminated employees from CMS' premises;
- User access is restricted using the least privileged, need to know concept;
- Access authorizations are approved by management, documented by standardized processes and retained for auditability per CMS policy;
- Procedures exist for revoking system accesses;
- Periodic reviews of the access authorizations by the Business Owner;
- Security managers review access authorizations and resolve any issues with the Business Owners;
- Audit trails are in place to track and hold users responsible and accountable for their activities; and
- Incompatible functions have been identified and different individuals are assigned to perform them.

The Evaluator shall validate the following:

- Appropriate personnel are assigned to plan for IS throughout the System Development Life-Cycle (SDLC);
- Personnel roles shall be clearly defined, and individual duties clearly established; and
- Appropriate personnel shall be assigned to perform specific security-related functions during each phase of the SDLC.

4.4.3. Authorize Processing

Obtain the date of authorization, name, and title of the management official responsible for authorizing processing of the system. If the system is not yet authorized, obtain the name and title of the management official requesting the authorization processing.

5. INTERVIEWS

As a part of executing the test scripts, the Evaluator shall conduct interviews with key staff members of the system support team to determine how the documented policies and procedures are followed. The key point of the interview process is to ensure that the processes conveyed by the interviewee are the same processes that are documented for the information system. Any gaps in the validation process will be reported in the findings report based on the *Reporting Procedures*.

Interviews are an integral part of the verification and validation of documented procedures as part of the assessment. In addition, during or after the review of relevant documentation it may be necessary to interview key personnel for further clarification or additional information. Prior to the interviews, review the SSP and/or IS RA to validate that all of the required functions are defined and addressed adequately. The system and/or application assessment plan and test scripts shall include assessment procedures to validate that the roles are staffed appropriately. Approximately a third of the test scripts are devoted to interviewing the relevant personnel experienced in each Security Control Family.

For interviews conducted by the Evaluator, the name and organization of the interviewee shall be recorded as well as the date, time and location of the interview. The records of the interview will assist in the validation of the testing process once the assessment has been completed.

The Test Scripts are written to guide the interview process and ensure the appropriate staff are assigned, trained and executing their responsibilities. The list of typical roles and responsibilities that follow is meant as a guide to assessing security personnel roles and their functions within CMS:

- Senior Management has the ultimate responsibility for the security of CMS' information systems. In order to support CMS' mission, it is management who sets the goals, priorities and objectives for an IS plan. It is also a management responsibility to be committed to the security plan and lead by example.
- The CMS System Administrators team controls day-to-day computer security activities. These individuals are tasked with coordinating all computer security-related issues between the various elements within and without CMS.
- Business Owners are responsible for a business function and its supporting system. These managers usually have a technical support staff to assist them in implementing the management, technical and operational security controls. In larger computer systems, a security officer may assist the system and/or application manager.
- System Developers / Maintainer design, operate and manage computer systems. They concern themselves with the implementation of the technical aspects of computer security. They are also responsible for day-to-day administration ensuring the availability of their systems and guarding against, and assessing, threats to the system.
- Telecommunications staff is responsible for providing communications services including data, voice, fax and video. They have responsibility for the communications systems in much the same way the system developer / maintainers have for their systems.

5.1.1. Relationships and Gaps

In order to ensure that all the required security functions are being performed, review all the relevant documentation gathered, together with the results of interviews, and determine if any gaps exist in the coverage. This may occur when roles and responsibilities are not clearly defined or when a particular security function has been overlooked completely.

The same person should not perform more than one of certain systems' support functions. The lack of independent oversight and verification can allow security controls and audit procedures to be compromised or bypassed, placing the system at risk. The system support functions include, but are not limited to, the following:

- Network Administration;
- Data control;
- Quality Assurance / testing;
- Data security;
- IS management;
- Data administration;
- System design;
- Production control and scheduling;
- Computer operations;
- Systems programming;
- Library management / change management; and
- Application management.

Certain combinations of transaction processing functions, if performed by the same individual, create the same of risk of compromise. Security controls and checks can be by-passed due to the lack of independent verification or oversight. Specifically, the following combinations of functions should be segregated:

- Data entry and data verification;
- Data entry and the reconciliation of input data to output;
- Supervisory authorization functions and data entry (e.g., having the authority to permit a rejected entry to continue that would normally require a supervisor to review because the entry exceeded some limit); and
- The same individual completing the input for vendor invoices / purchasing and receiving purchase data is an example of incompatible input processing functions.

Since each application and project staffing is unique, the potential combinations of incompatible business functions vary. It is therefore important for the Evaluator to understand the business mission in order to be able to identify incompatible duties and responsibilities.

6. SECURITY CONTROL ASSESSMENT

The Evaluator shall perform active testing of the information system security controls to assess their effectiveness and to identify gaps with the documented controls. Technical testing shall conform to NIST SP 800-42, *Guideline on Network Security Testing*, and NIST SP 800-115, *Technical Guide for Security Testing and Assessment*, guidance. The Evaluator shall follow a documented methodology for technical testing to ensure that the results can be reproduced by the Business Owner or their technical support staff, can be verified by a third party, and can be validated by CMS Management for use in other assessment activities.

The Evaluator shall document any discrepancies between the documented controls and the implementation of the technical control within the production environment, as well as any vulnerability in the implemented technical controls, as a finding in the assessment report as described in the *CMS Reporting Procedure for Information Security Assessments*.

6.1. IDENTIFY TEST ENVIRONMENT

The Evaluator shall identify the test environment and the targets within the environment that are relevant to the scope of the assessment.

6.1.1. Infrastructure

The infrastructure components typically include all of the network and computing resources not otherwise associated directly with a MA. This typically includes routers, switches, firewalls and the Intrusion Detection System (IDS). In some cases, infrastructure may involve a survey of desktop systems that are managed at the infrastructure level.

6.1.2. Applications

CMS employs tiered application structures in support of its business missions based upon hardware and software configurations. Most CMS applications rely upon two types of tiered structures known as “Two-tiered” and “Three-tiered”. A third type of application environment exists, as defined by CMS, known as “Mainframe”.

Two (2)-tier applications typically involve only a client and a server. The client portion of the application interacts directly with a supporting server system, which provides queried data based on the business function of the system. Testing in a two (2)-tier environment typically involves an evaluation of the server components and a survey of the client application, not the client host.

Three (3)-tier applications typically involve a client, middle-ware components, and a server. The middleware components may include a web-server, business logic component, or other data analysis function that regulates activity between the client and the server. Testing an application supported by the CMS three (3)-tier architecture requires the Evaluator to examine components in all three layers: the Presentation Zone, the Application Zone and the Data Zone. Targets shall be selected within these zones in a manner that demonstrates the continuous protection of traffic across all layers.

The “Mainframe” structure may be a blend of the tiered approaches. Some Mainframe applications reside within the database layer where the mainframe handles the data, the queries and the presentation. Other mainframe applications are configured to handle queries as background processes and report and/or update a data store also residing on the mainframe. Testing mainframe applications requires the Evaluator to:

- Examine the controls of the components over the application such as user access to the various types of transactions and the data; and
- Review authentication and authorization controls that may lead to the circumvention of existing controls specific to the application.

Applications can inherit risks and controls from the GSS. The Business Owner and Facilitator shall be aware of these risks and controls and how those risks and controls relate to their application. Any risk, control or lack of controls inherited from the GSS that creates vulnerability for the application, the Business Owner shall document and determine if the inherited risks are acceptable risks.

Identify Base Technologies

The Evaluator shall catalogue all the application technologies (e.g., Visual Basic, Java, SQL Server, WebSphere, etc.) that support the application processing followed by research of each of the technologies to determine potential current weaknesses that an application may inherit simply by incorporating the technology.

Identify Application Components

The Evaluator shall divide the application into its basic components. These include those components intended for workstations, servers, operating systems, network infrastructure, users, administrators and the application code itself.

Research Known Vulnerabilities

Based on the identified test environment, the Evaluator shall seek out known vulnerabilities affecting all aspects of the information system implementation. These include all published or generally known defects (bugs) and exploitable deficiencies in the operating system, web server, application server and other third-party components. Most of these vulnerabilities have existing patches, but hackers often exploit systems where patches have not been applied in a timely fashion.

6.1.3. Data Center

A Data Center assessment generally involves a review of the infrastructure and GSS and may be covered under infrastructure testing, however the scope may also identify specific applications hosted by the Data Center that are to be tested. The scope of Data Center testing will differ slightly from Infrastructure testing and the scope of the test will determine which targets within the Data Center, which are available to the Evaluator for the assessment.

6.2. DEFINE ASSESSMENT PROCEDURES

The Evaluator shall define a repeatable assessment procedure to ensure that assessment results, if questioned, can be validated by a third party.

6.2.1. Analyze Prior Test Results

The Evaluator shall review prior assessment results in an effort to understand past findings and any potential trends that merit investigation.

The Business Owner shall provide any CAP documentation for prior findings that are still in an open status in the CISS tool.

6.2.2. Identify Relevant Tests and Tools

The Evaluator shall identify the relevant tests and the tools that will be used to complete the assessment. The tests must reflect the relative priority of the security control categories (as determined during the Business Process Review). Testing shall focus initially on the categories of greatest priority.

Relevant tests shall include procedures to verify and validate the effectiveness of the documented management, operational and technical security controls and methods to discover and identify procedural and technical vulnerabilities and threats not documented within the system documentation.

After identifying the relevant tests to be performed, the Evaluator shall identify the tools that will be employed to complete each test. Tools may include technical software, such as port and vulnerability scanners, code scanners, as well as interview questionnaires and other non-technical instruments that may be employed to gather information, identify vulnerabilities, and assess IS.

Many of the automated testing utilities mimic the signs of attack and/or exploit vulnerabilities. As part of the tool selection process, the Evaluator shall identify any of the proposed tools that may pose a risk to the computing environment. The Facilitator shall ensure that the Business Owner has approved any tests that may pose a risk to the CMS environment; likewise, the Facilitator shall notify any managers that may be affected by testing, including the infrastructure manager, to ensure that they are aware of testing. Prior notification by the Facilitator shall enable affected managers to prepare their contingency plans and will minimize the risk of delay in completing test procedures.

Example: The Evaluator proposes to perform infrastructure network scanning within the Data Center to evaluate the network devices. Testing may be authorized by the Business Partner CIO, but only under the following conditions: (1) testing is permitted only outside of normal facility business hours; and (2) the scanning tools will be configured so they do not affect any after-hours processing tasks adversely.

6.2.3. Inventory and Validate Components

The Evaluator shall review the components inventory, as documented in the SSP or the RA, and shall validate it against the actual target environment. The validation process may include personnel interviews in addition to automated scans and manual test procedures.

6.2.4. Define Sampling Methodology

In most cases, it is unrealistic to test every component of an information system. In such cases, the Evaluator shall perform testing by observing a selected percentage of the entire population. This selection process is called *sampling*. A statistically valid representative sample provides confidence that the findings are systemic, not random, by taking into account the factors of breadth and size.

- 1) **Breadth:** Breadth of the sample assures that the testing covers a significant, representative cross-section of the population 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; and
 - 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.

When sampling is used, the Evaluator shall provide the Facilitator with a documented sampling methodology to ensure the results can be reproduced, verified and validated independently.

6.3. PERFORM SYSTEM TESTS

During the assessment of system controls, the Evaluator shall record the results of each validation process item on the approved test script document. The completed test scripts serve as a written record of the test process, and acceptance of the test results. For each element of the test process, the following items shall be recorded within the test script:

- Pass or fail assessment;
- Source of the documented control; and
- Key analysis points made by the Evaluator.

Test script notations shall also identify the Evaluator, by name or by initials.

The Evaluator shall retain all assessment tool outputs, test results, including notes, communications, documentation and related working papers, during the performance of system

tests and the vulnerability discovery process. This includes the capture, documentation and retention of information sufficient to demonstrate the existence of the vulnerabilities discovered through the testing process. This information may include, but is not limited to, working papers, screenshots, automated scan results, and e-mail communications. The Evaluator shall provide all test results to the Facilitator in accordance with the *CMS Reporting Procedures for Information Security Assessments*.

6.3.1. Discover Technical Vulnerabilities

Technical vulnerabilities may be discovered through a broad range of tools and testing procedures. In order to ensure that the test method used can be reproduced by CMS or by other third-party reviewers, the Evaluator shall document each test performed and the tools used.

Test procedures should only demonstrate that the vulnerability does or does not exist. Unless expressly authorized by CMS Management, the Evaluator shall ensure that all testing tools are configured to minimize the potential to disrupt system or business operations. The Facilitator may be required by CMS Management to review all testing tool settings before test procedures are executed within the CMS or CMS Business Partner environments.

The discovery process typically involves the execution of an attack upon the system being tested. The results from the attack may confirm a suspected vulnerability, or may expose other vulnerabilities to be targeted. The execution of an attack consists of several phases beginning with the Planning phase. For the Planning phase of the discovery process, it is important that testers understand what is to be tested and how. It is the Business Owner's responsibility to ensure that system boundaries and scope of testing are clear and well articulated. It is the tester's responsibility to use tools and techniques appropriate to the technical demands of testing, and to the environment in which testing is to take place. All of these assumptions, along with a list of core applications that testers expect to employ during testing, must become part of the final report.

During the Discovery phase, testers will determine those systems / networks to which they have logical access. This phase is where testers determine which systems or networks to target for more specific attacks based on testing objectives. For example, many testers employ what is known as a 'Ping Sweep' on a network segment in order to determine which hosts respond to Internet Control Message Protocol (ICMP) packets. This could be a fair measure of the number of hosts on that segment.

Once a set of targets is identified in the Discovery phase, testers may move on to the Attack phase, where they attempt to gain access to protected resources or escalate their user privileges, browse the system for interesting information, or install hacker tools that aid in any of the aforementioned attack methods. Another attack method, system disruption, is possible, but virtually never included, as part of testing.

Gaining access to system resources could be as simple as accessing a directory on a system that is not meant for public use. Testers will adjust their attacks according to the operating systems in use, the network architecture and the system architecture. They will attempt to browse directories, use applications and access networks and systems to which they may or may not have explicit permission. Detailed notes of methodology used and the results generated will be in the final report.

Escalation of privilege is another attack method that will be used by testers. Again, depending upon operating systems in place, testers will use tools and methods in order to increase their privilege levels on the network.

Testers will always browse any system to which they obtain access. They will be looking for any sort of sensitive information that is not reasonably protected from casual disclosure. This phase of testing may proceed through several iterations corresponding to the escalations of privilege testers attain.

Once inside a system, many attackers are tempted to plant malicious software agents on the hosts they breach. Many of these agents are simply back doors into the system, or provide a means for an attacker to cover their tracks. Other software agents are more malevolent such as logic bombs or keystroke loggers. These pose a direct threat to the confidentiality, integrity and availability of sensitive information.

Whatever methods testers use during testing, a methodology is retained for inclusion in the final report. Full results of testing, along with testing notes, will be included as well.

The following list provides some common test procedures and techniques that the Evaluator may employ for the technical assessment of different environments:

- Infrastructure:
 - Evaluate firewall rule set
 - Evaluate router configuration
 - Attempt to alter firewall rule sets and router configurations
 - Attempt to alter database management system settings
 - Attempt to alter packet structures to bypass security measures
 - Review server baseline configuration settings
 - Review workstation baseline configuration settings
 - Identify unnecessary ports and services

- Client-Server Application:
 - Evaluate application interfaces and user interface controls
 - Evaluate application input and output security controls
 - Attempt to gain access without a valid user account
 - Attempt to log-on with default and easily-guessed passwords
 - Attempt to access information resources outside the scope of the authorized user role to evaluate application privileges and user role configurations
 - Validate that “Read” and “Write” access is limited to only authorized resources

- Perform attempts to access application resources in the context of another user
 - Perform attempts to elevate access to a broader role
 - Review application-specific audit log configuration settings
 - Review application logs produced during testing to validate that application logging operates as required
 - Attempt to connect to management ports, services, and interfaces to review application administration and management connectivity
 - Test for buffer overflow conditions to confirm that forms limit user input
 - Evaluate application error handling and attempt to gather configuration information and other sensitive information from error messages
 - Inspect code and scripts for hard-coded passwords
 - Inspect code and scripts for the existence of back doors
 - Conduct user-role testing, based upon the role-related test mapping attached to the application assessment plan
 - Inspect code and scripts for vulnerabilities, coding weaknesses and potential buffer overflow conditions
- Web Application:
 - Attempt to take-over sessions created by other users
 - Attempt to restore old sessions without re-authenticating
 - Attempt cookie poisoning
 - Attempt to access hidden Uniform Resource Locators (URLs), including active server pages (ASP) or middleware components
 - Attempt to access and manipulate web scripts (Common Gateway Interface (CGI), ASPs, Java Server Pages, Cold Fusion, Perl, etc.)
 - Attempt to inject commands into web requests and submissions that can be used to subvert the database management system or the host operating system
 - Attempt Cross-Site Scripting (XSS)
 - Attempt SQL command injection
 - Attempt to manipulate HTML form submissions and hidden fields
 - Inspect code and scripts for sensitive information (hidden URLs, IP addresses, server names, SQL commands, etc.)
 - Data Center:
 - Evaluate physical security to the Data Center floor and infrastructure equipment
 - Review physical access controls
 - Attempt social engineering strategies to gain access to infrastructure areas, rooms and devices (see [Appendix F – Social Engineering](#)).

The list provided is not exhaustive. The Evaluator shall have the requisite experience with testing methodologies within the industry to affect an appropriate test for the environment as expressed in the assessment scope statement.

Assessment tools are constantly being updated. Appendix G identifies sources for the latest version of commonly used tools.

6.3.2. Discover Procedural Vulnerabilities

During the technical evaluation of system controls, the Evaluator may identify discrepancies between the implementation of a technical control and the mitigation expectation of the technical control. The Evaluator shall identify these discrepancies as a Procedural vulnerability. Procedural vulnerabilities may also be identified through interviews with system support staff, following the scripted interview questions, and through comparisons of implemented controls with the documented details of the controls and as a result of the documentation review if documented controls are either insufficient to mitigate risk or are non-compliant.

6.4. VALIDATE VULNERABILITIES

All vulnerabilities identified during the assessment process shall be reported to the Facilitator whether they fall within the verified test sample or not. The Evaluator shall not report vulnerability as a finding unless the vulnerability has been verified for the tested sample. The Facilitator may determine that vulnerability is severe enough to be included as a finding in the report regardless of being outside the verified sampling. Automated vulnerability scanning tools periodically report “false positive” and “false negative” results.

- A false positive occurs when a vulnerability does not exist but the assessment results come back as positive

Example: A tool indicates that an identified system vulnerability is sufficiently mitigated and cannot be exploited. Manual validation of the vulnerability shows that, while the automated scan provided correct information, the vulnerability is still easily exploited.

- A false negative is when a vulnerability exists but the assessment results come back as negative

Example: A tool reports an operating system version and an application version that, when combined, is shown to open a port that may be exploited. Manual validation of the vulnerability shows that, while the automated scan provided correct information, other controls are in place to mitigate the risk by blocking the exposed port.

Scanning tools generally rely upon system and application version numbers, rather than direct exploitation of a vulnerability, to determine whether a risk exists. This is why a manual validation is necessary.

6.4.1. Manually Validate Documented Controls

The Evaluator shall validate the technical controls of the system through the execution of automated and manual test procedures. Validation procedures may require the examination of an application user interface, device-specific controls (i.e., authentication mechanisms, session control, access restrictions, communications protection, audit logs) and, if necessary, the review of application source code and device configuration settings. Manual validation of technical

controls may also require that the Evaluator engage in personnel interviews with technical staff supporting the system.

Manual validation for web-associated vulnerabilities, text window access vulnerabilities, and similar vulnerabilities may require user intervention to exploit. The Evaluator shall, based on the expertise of the Evaluator, conduct validation exercises to determine whether an identified vulnerability meets the following criteria:

Valid: The vulnerability may be exploited by the Evaluator and, therefore, may exist. The Evaluator has not exploited the vulnerability directly in order to prevent any adverse affects to the system or the computing environment. Sufficient information exists to demonstrate that the vulnerability is exploitable.

Invalid: The Evaluator would not be able to exploit the vulnerability under current system conditions. The Evaluator collected and analyzed information sufficient to support the assertion that the vulnerability is not exploitable.

6.4.2. Inspect and Review Controls Manually

The Evaluator shall conduct manual review processes designed to test the security implications of people, polices, procedures and processes. The review may include the inspection of technology decisions supporting security control requirements. Other activities accomplished using manual inspections and reviews are documentation reviews; secure coding policies; security requirements; and architecture designs.

Manual inspections and reviews are one of the few ways to test the SDLC process and to ensure that there are adequate technical controls, policies and procedures in place to ensure that the integrity of the security controls is maintained throughout the system life-cycle. Manual reviews are particularly useful for testing whether or not people understand the security process, have been made aware of policy, and have the appropriate skills to design and implement the system security controls.

6.4.3. Verify Known Vulnerabilities

The Evaluator shall probe the information system using test examples to verify the known security flaws. Test procedures developed by the Evaluator shall confirm that vendor-identified, or other published vulnerabilities that may exist in the system code or configurations, have been appropriately mitigated by existing system security controls.

6.5. REPORT ASSESSMENT RESULTS

Guidelines for reporting assessment results are addressed in the *CMS Reporting Procedure for Information Security (IS) Assessments*. A summary of key points is provided in this section.

Technical findings will contain system-specific information about the weakness, including Common Vulnerabilities and Exposures (CVE) numbers and citations to other sources for information about a reported vulnerability. Technical findings relate vulnerabilities that may lead directly to an exposure of information assets.

Complete the “Description” section of the Business Risk template by documenting the technical details of the vulnerability, which include:

- 1) How the vulnerability was discovered and validated;
- 2) How the vulnerability could be exploited;
- 3) Who may exploit the vulnerability;
- 4) What systems (IP addresses) are affected by the vulnerability; and
- 5) The harm or damage that would occur if an attacker were to exploit the vulnerability.

The Evaluator shall describe the harm or damage that may occur if an attacker were to exploit the vulnerability in terms of the business impact to CMS. Specifically, the Evaluator shall identify what type of data is at risk, the sensitivity level of the data, and how the CIA of CMS information assets may be affected.

6.5.1. Report a Critical Vulnerability

A critical vulnerability includes any High-risk weakness where the threat exposure is also considered High. The combination of High risk and High exposure indicates that the security controls do not reduce the severity of impact effectively if the vulnerability were to be exploited. The situation requires immediate mitigation by the Business Owner to fix the weakness or reduce the threat exposure of the system.

If, during the assessment, a critical vulnerability is discovered and confirmed to exist, the Evaluator shall report the finding immediately to the Facilitator with documentation that describes the vulnerability and any suggested corrective actions. The Facilitator shall notify the Business Owner to confirm the criticality of the finding. Once the criticality of the vulnerability is confirmed, the Business Owner shall notify EASG and CMS Management of the critical vulnerability and begin appropriate mitigation efforts.

If there is any question as to whether vulnerability is critical and requires immediate notification, the Evaluator shall err on the side of caution and report the vulnerability immediately to the Facilitator.

6.5.2. Prepare Final Deliverables

The Evaluator shall furnish all of the automated test results and notes from the validation and verification efforts as part of the Final Assessment Report Package, in accordance with the *CMS Reporting Procedure for Information Security (IS) Assessments*. All files should clearly indicate the method used, the tool used to generate the result, the name and company of the Evaluator, and any additional analytical assessment of the results.

APPENDIX A: ASSESSMENT PLAN INSTRUCTIONS

Instructions

Fill in the Assessment Plan Template in Attachment A with information appropriate to the engagement being planned.

1. Prepare

The Evaluator shall be expected to review, at a minimum, the IS RA and the SSP for the system being assessed in order to prepare the Assessment Plan. The Facilitator and the Business Owner shall have an opportunity to comment on the Assessment Plan and request that the Evaluator update, add or delete Assessment procedures. The Facilitator shall perform the final review and authorize the Assessment Plan before the start of any assessment activities.

2. Identify Controls

Based upon the documented security control requirements and the system security level, the Assessment Plan shall identify the priority each of the seventeen (17) security control families, as well as e-authentication, described in the *CMS IS Acceptable Risk Safeguards (ARS)*. Prioritization of assessing the control families shall consider the following factors:

- (1) Sensitivity requirements of the information system under review;
- (2) Criticality requirements of the information system under review;
- (3) Technical and Business risks documented within the IS RA; and
- (4) Potential harm that may result if the controls for the control family are found to be inadequate or ineffective.

As a general rule, certain control families, such as Access Control (AC) and Identification and Authentication (IA), will be a higher priority than other categories, such as Awareness and Training (AT) and Maintenance (MA). For example, Application “A” may be a financial application supporting a high-profile business function distributed among multiple sites. In the case of Application “A”, which has a high system security level, ineffective security controls in the AC category may directly cause significant financial loss. Ineffective controls in the AT category, however, assuming that other control categories are sufficient, would probably not cause the same level a risk of financial loss.

In most cases, the actual prioritization of control families will be system or application-specific. The individual sensitivity and criticality requirements of the business function supported by each system or application, the known business and technical risks, and the potential harm (in terms of financial loss, political damage, public embarrassment, information disclosure and legal consequences) that CMS might experience will drive the control family prioritization process.

In order to ensure that time and other resources are allocated to the most critical control families, the Assessment Plan should include that the first families to be evaluated and validated shall be the high-priority controls which, if not adequate and effective, may result in the greatest potential

harm. Moderate priority controls shall be evaluated during the subsequent assessment phase, and Low-priority controls during the last phase.

3. Document Processes and Procedures

The Assessment Plan documents the processes and procedures that are to be executed during the assessment. The Assessment Plan shall include the relevant assessment procedures identified during the previous step, and assign / apply relevant tools, methods and personnel to achieve the assessment objective. The Assessment Plan shall define a progressive methodology for conducting the assessment. The first phase of testing is conducted with the least information and access, and subsequent phases of testing involve greater knowledge of the technical application and increased access. For example, the first phase of testing may involve remote testing from the perspective of an unauthorized person. The next phase may then involve on-site testing from the perspective of an unauthorized person. The following phase would then involve on-site testing from the perspective of an authorized internal user, and the final phase would involve review of information or access provided to the Evaluator by CMS. This progressive methodology is also referred to as an “outside-in” strategy.

The Assessment Plan shall include a requirement whereby the Evaluator validates the effectiveness of security controls documented within the SSP / IS RA. Specific procedures for conducting these validation checks will be documented within the test scripts. The Assessment Plan shall also include the processes to be employed to discover, identify and validate procedural and technical vulnerabilities in the application. These processes may include, but are not limited to; port scanning, vulnerability scanning, password cracking / discovery, manual penetration testing / access attempts, and technical review, analysis and evaluation based upon interviews and documentation review. When a second or deeper level of application security testing is required, an actual Application Source Code Review shall be conducted see Appendix E: Application Source Code Review. The Assessment Plan shall also include requirements to re-test open vulnerabilities, to validate completed corrective actions and to validate the application component inventory.

4. Define Role-Related Tests

The Assessment Plan shall define a set of role-related tests that will be conducted. The purpose of the role-related testing is to validate that proper access permission and restrictions are assigned for each of the application user roles. Role-related tests shall be assigned to each of the relevant application user roles. For example, the Evaluator, in developing the Assessment Plan may define seven (7) role-related test procedures (i.e., attempt to add user, attempt to change password, attempt to access a certain database, etc.). The role-related tests shall then be assigned to each of the application user roles, based upon the access permissions and expectations associated with each user role. The types of role-related tests to be conducted and the identification of application user roles shall be based upon the application type, user interface and results / findings from the Business Process Review. The following table is an example of the role-related test (RRT) mapping:

Table 1: Roles and Role-Related Tasks

| Roles | RRT-1 | RRT-2 | RRT-3 | RRT-4 | RRT-5 | RRT-6 | RRT-7 |
|----------------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| Administrator | - | - | X | X | - | X | X |
| Help Desk | X | - | X | X | X | X | X |
| User Level II | X | X | X | X | X | X | X |
| User Level I | X | X | X | X | X | X | X |
| Unauthorized User ID | X | X | - | - | - | X | X |
| No User Account | X | X | - | - | - | X | X |

5. Identify Prior Test Results to be Include

The Assessment Plan and test scripts shall be expected to reflect the reuse of additional assessment results that address the inheritance of security controls related to the scope of the assessment. For controls that can be inherited from other sources, the Evaluator shall need proof that a prior assessment has been performed recently and will need to determine if prior testing was adequate. This may include a technical analysis of the prior test scope and results to determine if the previous security testing was technically sufficient to address the control inheritance by the system being assessed. If prior testing was adequate, the Facilitator shall opt to use these results in lieu of additional testing for the inherited controls.

6. Identify Assessment Tools

Table 2: Assessment Tool Identification

| Operating System (O.S.) | Tools by O.S. |
|---|---|
| <p>LINUX</p> <p>Basic Linux functionality: Awk, Grep, Cat, vi, emacs, Perl USB support for secure memory sticks Web browser, wireless support</p> | <p>LINUX</p> <p>Nessus REGISTERED for full plug-in download, with a user name. NMap Nikto with SSL Support John the Ripper ADM's SNMP Scanner tnscmd.pl SNMP Walk Snort Cisco Global Exploiter Cisco Torch THC</p> |
| <p>WINDOWS XP/2000</p> <p>Windows basic functionality:</p> | <p>WINDOWS XP/2000</p> <p>Nessus client</p> |

| Operating System (O.S.) | Tools by O.S. |
|--|---|
| Word, Excel, Access Web browsers (IE and Firefox – current versions) Terminal Services | AirCrack Brutus Cain&Abel I0phtcrack ISS Database Scanner NBTdump MAC Makeup WebScarab Metasploit framework Oracle 10 admin tools LDAP Miner Windows administration tools Microsoft Baseline Configuration Analyzer Ethereal and/or WireShark NetStumbler SusperScan X-Scan THC Hydra GFI LANGuard Network Security Scanner ISS Internet Scanner (latest version) Wikto |

NOTE: The above lists of tools are to suggest not that ALL of the tools will be used, but what are necessary to have on-hand in response to positive vulnerability scans. Each engineer also may maintain an individualized list of preferred tools, based upon, but not limited to, the top 100 security tools listed at <http://sectools.org/>.

7. Define POA&M Support Activities

The Evaluator shall include support of the POA&M following the submittal of the final report. This support includes, but not limited to, the following:

- Review CAPs prior to submittal to CMS through the CISS tool;
- Feedback in response to the Facilitator regarding adequacy to mitigate risks; and
- Support and clarification meetings for recommended/suggested remediation.

8. Create Preliminary Schedule

NOTE: Table 3 is an example of a suggested Assessment Plan schedule and dates are subject to change to accommodate staff availability and scheduling issues.

Table 3: Preliminary Schedule

| Description | Responsible Party | <Assessment name> Date | Timing Relative to On-Site | Timing Relative to Final Package Delivery |
|---|---|------------------------|----------------------------|---|
| CMS delivers notification (Letter, RoE, & Pre-requisites request) | CMS FACILITATOR | 11/6/09 | 8 weeks prior | 14.5 weeks prior |
| Introductory Call | <Evaluator> CMS FACILITATOR | 11/20/09 | 6 weeks prior | 13.5 weeks prior |
| Delivery of RA & SSP | Owner | 11/24/09 | 5 weeks prior | 12.5 weeks prior |
| Deliver Draft Assessment Plan | <Evaluator> | 12/4/09 | 4 weeks prior | 11.5 weeks prior |
| Hold Draft Assessment Plan Meeting | <Evaluator> CMS FACILITATOR Owner | 12/11/09 | 3 weeks prior | 10.5 weeks prior |
| Deliver Final Assessment Plan | <Evaluator> | 12/18/09 | 2 weeks prior | 9.5 weeks prior |
| Delivery of relevant system, policy and procedure documentation | Owner | 12/18/09 | 2 weeks prior | 9.5 weeks prior |
| <Evaluator> <test> team preparation | <Evaluator> | 12/25/09 | 1 week prior | 8.5 weeks prior |
| On-site | <Evaluator> Owner | 1/1/10 | ... | 7.5 weeks prior |
| Analysis | <Evaluator> | 1/12/10 | 1 week after | 5.5 weeks prior |
| Delivery of Draft Report | <Evaluator> | 1/24/10 | 2.5 weeks after | 4 weeks prior |
| Draft Report Meeting | <Evaluator> CMS FACILITATOR Owner | 1/31/10 | 3.5 weeks after | 3 weeks prior |
| Delivery of CMS & Site Comments | CMS FACILITATOR Owner | 2/7/10 | 4.5 weeks after | 2 weeks prior |
| Delivery Final Report | <Evaluator> | 2/14/10 | 5.5 weeks | 1 week prior |

| Description | Responsible Party | <Assessment name> Date | Timing Relative to On-Site | Timing Relative to Final Package Delivery |
|-----------------------|-------------------|------------------------|----------------------------|---|
| | | | after | |
| Final Package | <Evaluator> | 2/21/10 | 6.5 weeks after | ... |
| Complete Book & Close | <Evaluator> | 2/28/10 | 7.5 weeks after | 1 week after |

9. Identify Necessary Resources

Resources for a test can include, but are not limited to, the following:

- Evaluator staff;
- Testing equipment (hardware, software, etc.);
- CMS and target site personnel (security related the target); and
- Facilities (conference room, workstation, a secure means to store documents, equipment, etc.).

10. Identify Test Site Location

The Assessment Plan shall identify and provide the full address of the host location to include the point of contact name, telephone number and location on site.

11. List Contact Information

The minimum information that should be provided within this section relevant to CMS staff is: Business Owner; System Developer/Maintainer; SSP and IS RA Author(s); Individual(s) responsible for security; and Component ISSO. For each position listed the following information is required:

- Name
- Title
- Organization
- Address
- Mailstop
- City, state, zip
- Telephone
- E-mail
- Emergency contact

The minimum information that should be provided within this section relevant to the Evaluator and staff to be on-site is: Project Manager; On-site Test Lead; and Evaluators. For each position listed, the following information is required:

- Name, Title
- Organization
- Address
- City, state, zip

- Telephone
- E-mail

APPENDIX B: TEST SCRIPTS

Instructions

The Facilitator shall provide the Evaluator with CMS test scripts to serve as a baseline for the objectives applicable to the assessment. The Evaluator shall modify the test scripts further to support the Assessment Plan by providing detailed criteria to follow for validating the implementation and effectiveness of documented security controls based on the security service families involved.

The CMS Security Assessment Test Scripts (*e.g.* ST&E, FISMA Assessment (FA), *etc.*) are based on the required security controls from NIST SP 800-53A, the *CMS Policy for the Information Security Program (PISP)*, the *CMS IS ARS* and the *CMS Minimum Security Requirements (CMSRs)*. Additional references to the Government Accountability Office GAO 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 HIPAA, and the IRS Publication 1075 *Tax Information Security Guidelines for Federal, State and Local Agencies*. If a business function is not subject to a particular requirement, for example FISCAM, those minimum security requirements are encouraged but not mandatory.

The scripts have a well-defined organization and structure which has been based on the security controls as presented within NIST SP 800-53A. In addition, the format is designed to afford the testers 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 two-character identifier for the Risk Assessment family is “RA”.

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.

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, CMS IS ARS, 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:

Control

The control is the documented policy statement(s) for the information security program at CMS for that particular security service family. The statements are taken directly from the PISP.

Guidance

This row contains information which is taken directly from NIST SP 800-53A, Supplemental Guidance section for each control. This is the additional assurance requirement identified for the particular control.

Applicability

The column corresponds to the References column and means that the particular control satisfies the stated references. For example, if in AC-1, applicability states "All", this means that the assessment objective being met complies with the requirements from ARS AC-1, FISCAM, HIPAA, IRS-1075, NIST 800-53/53A AC-1, and PISP 4.1.1.

References

These are the various requirements related to the control that have been identified such as the ARS, FISCAM, HIPAA, IRS-1075, NIST 800-53/53A and the PISP.

Related Controls

This cell documents any of the other controls that are associated with the assessment control.

Assessment Procedure

An assessment procedure consists of *objectives*, each with an associated set of *methods* and *objects*. The application of an assessment procedure to a security control produces *findings*. The findings are the deficiencies resulting from applying the methods to the objects when assessing if the implemented control(s) meet the objective and are used subsequently in determining the overall effectiveness of the security control.

Objectives

The objectives include a set of *determination statements* related to the particular security control. These statements are linked closely to the content of the security control requirements, i.e., the security control functionality. The tester shall use the various test methods to determine that the objective is being fulfilled by the implemented control.

Methods

The methods are the actions to be applied by the assessor/tester against each implemented control and include the following:

- Examine,
- Interview, and

Test (meaning a functional test).

Objects

The objects are the entities against which the methods are to be applied, i.e., the artifact(s) to be examined, the person(s) to be interviewed and the system(s) to be functionally tested.

Enhancement

In addition, each of the controls within the families has an enhancement control section, which documents the corresponding control enhancement from NIST 800-53/53A, ARS and FISCAM. The enhancements are numbered based on the following configuration:

- a. The control family with each numbered row indicating a base control (the NIST SP 800-53 numbering scheme is used, i.e., the security control family acronym followed by a sequential number, e.g., AC-1, AC-2, etc.)
- b. The controls, which have the required enhancements or amplifications, use the numbering scheme from the ARS, e.g., an enhancement numbered "**AC-2(0)**" is used when amplification or defining of periodicity of controls indicated in the ARS. It should be noted that enhancements "0" are from the baseline control in the PISP.
- c. The additional controls and enhancements unique to CMS are distinguished by the characters "CMS-" followed by a sequential number in the base control and/or enhancement. Thus, "**AC-2(CMS-4)**" is the fourth CMS unique enhancement to control AC-2.
- d. There are additional enhancement controls unique to FISCAM requirements. These are identified by "FIS-" and followed by a sequential number for the enhancement. "**AC-1(FIS-1)**". This is the first control in the Access control family, first enhancement from FISCAM.
- e. The additional enhancement controls unique to CMS are distinguished by characters "DIR-" followed by a sequential number in the enhancement. "**PE-3(DIR-1)**". This would be the first control in the Physical Environmental family, first enhancement from CMS.

Requirements Met?

This column enables the assessors/testers to incorporate their overall results.

- Mark "Y" for a "Yes" when the requirement has been fully met and initial for each assessment 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.

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.

APPENDIX C: RULES OF ENGAGEMENT (RoE) INSTRUCTIONS

Instructions

Below are boilerplate examples of each section of the RoE. These examples should be used and modified according to the specific engagement to develop an individualized and unique RoE.

1. Background and Statement of Purpose

The Centers for Medicare and Medicaid Services (CMS) of the United States Department of Health and Human Services is the Federal agency responsible for administering the nation's Medicare and Medicaid programs. In this capacity, CMS is responsible for the payment of over \$400 billion each year for medical services rendered to nearly ninety (90) million program beneficiaries and recipients. CMS contracts with approximately sixty (60) business partners to process claims for reimbursement for medical services rendered under the Medicare program, and work in all fifty (50) states in the management of the Medicaid program.

In the course of administering and delivering public programs and services, CMS collects, stores, processes and transmits sensitive personal, intergovernmental and proprietary information. A robust IS program is essential to the timely, consistent and proper completion of the CMS business mission. Stringent security controls and practices are required to preserve and protect the confidentiality, integrity and availability of the information resources that support the Medicare and Medicaid business functions.

A critical component of the CMS IS program is security assessments to verify that proper security controls are implemented, in accordance with legal, regulatory and policy requirements. The testing includes an assessment of the management, operational and technical controls.

The Rules of Engagement (ROE) governing the assessment process is established within this document. The ROE defines the scope of the assessment process, the assessment period, the types of assessment that will be performed and management requirements.

2. Administrative

2.1. Time-frame

Certification testing is scheduled to begin on [date]. It is expected that the testing process will be completed by [date]. All testing activities shall be conducted during standard business hours between 8:30 AM and 5:00 PM. If the Evaluator requires testing to be conducted beyond these hours, management authorization must be obtained.

The schedule for testing shall be provided, and the timeline for each site visit shall be completed in the CMS Penetration Test Site Schedule. CMS shall contact each site to verify that the time set forth will be acceptable to all parties.

2.2. Points of Contact

Table 1: Points of Contact

| ROLE/CONTACT ELEMENTS | DATA DESCRIPTION |
|--|-------------------------|
| CMS Facilitator or Project Leader | |
| Name | |
| Title | |
| Name of Organization | |
| Address | |
| Address Line 2 | |
| City, State, Zip Code | |
| E-mail Address | |
| Telephone Number | |
| Emergency Contact | |
| CMS C&A Evaluator | |
| Name | |
| Title | |
| Name of Organization | |
| Address | |
| Address Line 2 | |
| City, State, Zip Code | |
| E-mail Address | |
| Telephone Number | |
| Emergency Contact | |
| Business Owner | |
| Name | |
| Title | |
| Name of Organization | |
| Address | |
| Address Line 2 | |
| City, State, Zip Code | |
| E-mail Address | |
| Telephone Number | |
| Emergency Contact | |
| System Developer/Maintainers | |
| Name | |
| Title | |
| Name of Organization | |
| Address | |
| Address Line 2 | |
| City, State, Zip Code | |
| E-mail Address | |
| Telephone Number | |
| Emergency Contact | |
| Information System Security Officer | |
| Name | |

| ROLE/CONTACT ELEMENTS | DATA DESCRIPTION |
|------------------------------|------------------|
| Title | |
| Name of Organization | |
| Address | |
| Address Line 2 | |
| City, State, Zip Code | |
| E-mail Address | |
| Telephone Number | |
| Emergency Contact | |

2.3. Resource Requirements

The CMS Evaluator shall provide qualified security testing personnel, equipment and materials necessary to complete the assessment procedures. The CMS Evaluator’s key personnel shall have suitable past experience in conducting assessments, and must have knowledge of CMS security policies, standards, guidelines and procedures.

To promote the efficient and proper completion of the ST&E process, the CMS Evaluator shall require that technical staff responsible for the regular management and administration of [system name] to be made available during the process. Technical staff shall be readily available to answer questions of technical nature, and to resolve any problems or difficulties the CMS Evaluator may encounter.

All security documentation, including the IS RA, the SSP, any local security policies and Standard Operating Procedures, the Disaster Recovery Plan, the Continuity Plan and a current network diagram shall be provided to the CMS Evaluator. The technical staff, on completion of the assessment, shall provide to the CMS Evaluator the Intrusion Detection System (IDS) results or a statement attesting to the IDS log file findings for analysis. In addition, the technical staff shall provide the incident handling procedures to the CMS Evaluator to determine the handling of a suspect incident if identified by the IDS.

2.4. Security Requirements

The CMS Evaluator shall comply with the information systems security requirements set forth in this ROE, the CMS IS Virtual Handbook (www.cms.hhs.gov/informationsecurity), and all local security policies not in direct conflict with CMS information security requirements. CMS policy takes precedence over local security policies.

All non-governmental employees of the CMS Evaluator shall meet personnel security / suitability standards commensurate with their position sensitivity level, and are subject to personnel investigation requirements. Access to government information shall be granted upon demonstration of a valid need to know, and not merely based upon position, title, level of investigation or position sensitivity level. All non-governmental employees of the CMS Evaluator are required to complete the proper security requirements, in accordance with the CMS and DHHS Personnel Security / Suitability Handbook. All CMS Evaluator personnel who shall be responsible for technical analysis of information systems are required to obtain a Level 5 Moderate Risk or Level 6 High Risk background investigations.

2.4.1. Handling and Storing Sensitive Information

The CMS Evaluator is required to handle, store, disseminate and dispose of any sensitive CMS information collected, shared or developed during the testing process, in a manner consistent with CMS security policy. Sensitive information may be shared only with individuals on a need-to-know basis. Proper security practices must be followed to prevent accidental or intentional disclosure of sensitive information.

On completion of testing, all materials collected or shared during the assessment process, in either electronic or hard copy format, must be disposed of properly. All electronic data and hard copy documents must be either returned to CMS or disposed of according to NIST SP 800 -88 Guidelines for Media Sanitization; If not return of the material is not required as part a contract then CMS must receive an attestation that all sensitive information related to this assessment was disposed of properly.

3. Scope of Testing

3.1. System Environment

[Define technical boundaries for certification task here]

3.2. Test Procedures

The CMS Evaluator shall:

- Schedule and conduct security testing, collaborating with CMS employees and the Business Owner as necessary.
- Provide an assessment Work Plan that identifies the objective of each test, pre-requisites that must be completed prior to the test, all test procedures that will be conducted, and expected results.
- Conduct only those test procedures that have been authorized mutually by the CMS Facilitator and the Business Owner.
- Notify the Assessment Facilitator and technical personnel prior to performing any testing. All tests shall be done with the full knowledge and authorization of CMS.
- Permit CMS, the Business Owner or technical personnel to monitor and observe test procedures.
- Cease all testing activities immediately at the direction of the Facilitator, or the Business Owner, or technical personnel.
- Notify CMS and the Business Owner of all software, programs, applications, utilities, scripts and other forms of tools that will be used to complete the security testing. No such tools shall be used without the express authorization of CMS and the Business Owner.
- Follow generally accepted industry and government testing standards.
- Perform all testing in a non-destructive, least intrusive manner. No Denial-of-Service test procedures or any other test procedures with the potential to cause widespread damage or disruption shall be performed.

- Maintain a test log and document all results.
- Verify the authenticity and validity of actual test results.
- Inform the CMS Facilitator and the Business Owner immediately if a serious vulnerability or defect is discovered, which poses an imminent danger to the system or network environment.
- Obtain mutual authorization from the CMS Facilitator and the Business Owner if it becomes necessary to modify or vary from any of the agreed-upon test procedures.
- Be able and available to reproduce any test result at the request of CMS or the Business Owner.

4. Work Product

The CMS Evaluator shall record all test results within the assessment Work Plan and within a test log. After completing the certification evaluation, the CMS Evaluator shall produce an assessment report, which will form part of the Certification & Accreditation (C&A) Package to be delivered to the CIO in accordance with the *CMS Certification & Accreditation Program Procedures*. The assessment findings shall be documented in the assessment report after the on-site and off-site testing has been completed. The assessment report shall be made available to the CMS Facilitator and the Business Owner for review, prior to final assembly of the C&A Package.

5. Assessment Impact Statements

It is CMS' intent to conduct the assessments with minimal impact upon the infrastructures that manage / own the systems. In an effort to accommodate the concerns of the Business Owner, CMS realizes that tests conducted on systems / networks may sometimes incur some degradation of bandwidth or system performance. In these cases, the CMS Evaluator may be asked to conduct the tests after the business hours, during the week or over the weekend to avoid impacting the users / customers during regular business hours (8 a.m. through 5 p.m., local time). The schedule of testing is to be determined before the visit and agreed upon by the CMS Facilitator, Business Owner and CMS Evaluator management.

In the unlikely event of an adverse effect on the underlying network, operating system, application or hardware, the CMS Evaluators shall adhere to a strict protocol to minimize the impact on mission-critical operations:

- Prior to any testing, emergency contact information will be given to all individuals authorized to halt the tests.
- Upon request of the Data Center, or CMS Partner management, or CMS Facilitator, the CMS Evaluator shall halt the current phase of testing immediately.
- Should there be a request to halt the current phase of testing, the Data Center or CMS Partner management Contractor shall contact either the on-site CMS representative, if available, and the Facilitator with the supporting evidence of degradation.
- Once the current phase of testing has been halted, the CMS Evaluator shall report to the CMS Evaluator Project Leader who shall then inform the CMS Facilitator of the interruption of testing and provide any information in regards to the nature of the tests conducted at the time of the request.
- The CMS on-site shall have the responsibility to research the issue and advise the CMS Facilitator or CMS Facilitator Back-up of the details of the problem.

- The CMS Facilitator shall then direct the CMS Evaluator as to the next course of action:
 - Resume the interrupted phase of testing;
 - Research and investigate the nature of the degradation with the intent to resume the phase of testing after determining measures that will prevent further degradation;
 - Resume the interrupted phase of testing during non-business hours as agreed upon by the CMS Facilitator, Data Center or CMS Partner and the CMS C&A Evaluator;
 - Continue with the new phase of testing; or
 - Cease all testing.

APPENDIX D: COMMON VULNERABILITIES

1. APPLICATION VULNERABILITY CLASSES

There are nine (9) classes of common security flaws that place the confidentiality, integrity and availability of an application at risk. These classes shall form the baseline for a vulnerability assessment. The flaw classes are:

1. Administrative interfaces;
2. Authentication & Access control;
3. Configuration management;
4. Information gathering;
5. Input validation;
6. Parameter manipulation;
7. Sensitive data handling;
8. Session management; and
9. Cryptographic algorithms.

Within these classes are a series of common vulnerabilities that can be identified uniquely.

Inadequate Identification and Authentication

Occasionally, users are not required to enter a password before accessing an application, which can result in an easily circumvented authentication process. This category also includes authentication of users who should be denied access.

Insufficient Access Control

When restrictions on what authenticated users are prevented from doing are not properly enforced, both malicious and inadvertent access to other users' accounts, viewing of sensitive data, or using unauthorized functions may occur.

Improper Integration of Application Components

The application integration process could leave "backdoors" or "security holes" that make it possible for users to bypass access controls, second-level identification and authentication, or other security controls. Improper integration could also enable the ability to read security data passed between components, including incorrect interfaces between the application and cryptographic mechanisms on which the application may depend.

Weak Passwords

Passwords that are too short, not changed frequently enough, easy to guess, or which may be defaults provided by a vendor place the system at risk.

Plain Text Communication of Sensitive Information

Unencrypted, or plain text information may provide a way to circumvent or bypass application controls; e.g., clear text transmission of user passwords. This places both the integrity and confidentiality of the application at risk.

Incorrect Reparsing of Data

Movement of data, without adequate security, into application components where data processing occurs, such as user-provided identification data passed between application and back-end server.

Susceptibility to Buffer Overflow

Application components in higher-level languages, such as C, C++, etc. may not limit the amount of input properly, thereby allowing the data cache buffer for the application to overflow. When it overfills, the excess data may leak into the processing cache where they can result in a Denial-of-Service or possible exploitation of the application.

Lack of Adequate Parameter Validation

Parameter manipulation occurs when input data (such as query strings or cookies and form fields) are manipulated to cause an unintended action to occur. Parameters should always be validated to ensure the proper formatting and length each time the parameter is passed to the application. If not done, attackers can manipulate parameters in order to create unexpected or undesirable events within the application. This validation is an essential part of session control.

Input Validation of Active Content Data

Insufficient validation could cause active content-based applications to execute unexpected processes and make the application vulnerable to “Cross-Site Scripting” (XSS). In XSS attacks, the application can be used to transport an attack to an end user’s browser or back-end systems, allowing the attacker to view session tokens, manipulate the remote workstation, or spoof or modify content in a way that the system does not expect or intend. This integrity check is part of Parameter Validation.

Acceptance of Meta Code Embedded Within Input Data

This vulnerability enables “stealth commanding”; i.e., the insertion of shell meta-characters in data input. An example is the character ‘!’ which is used to access the command history in some shells; particularly troublesome in tcsh, where ‘!’ can be used not just interactively, but in scripts. Another example is ‘|’ (the “pipe”) in Perl. Many Perl programs allow the user to input a filename, and then pass that filename to a program in a shell command. Because the shell’s interpretation of the characters is different from that of the Perl program, if the user includes ‘!’ (the “bang”) within the filename, the shell will attempt to execute the rest of the filename as a program. By including control string code (allowing the user to execute unintended actions) after the ‘!’ character, hidden debug code or developer-instituted backdoors may result in compromised security controls. This integrity check is also part of Parameter Validation.

Direct Command Injection

Acceptance of Illegal Characters in SQL Queries Database applications that do not correctly validate and/or sanitize the user input can potentially be exploited in several ways. These exploits include: 1) changing SQL values; 2) concatenating SQL statements; 3) adding function calls and stored-procedures to a statement; and 4) typecasting and concatenating retrieved data. All applications should be stripped (or cleansed) of any characters or strings that, possibly, could

be used maliciously. Failure to do so places the confidentiality (including privacy), integrity and availability of the application at risk.

Use of Relative Pathnames

The use of relative pathnames enables users to gather information about the directory structure and content of application systems that can be used to launch other types of attacks. With this knowledge, malicious users could access confidential information remotely or execute protected applications.

Remote Directory Listing

If no filename is specified at the end of the pathname, the system may simply list the full directory contents to the user, enabling a malicious user to gather information about the application for use in an attack. When coupled with improper access controls, this information could enable the release of confidential data.

2. ADDITIONAL COMMON VULNERABILITY SOURCES

In addition to the common security flaw classes, all individuals responsible for the security assessment process should be aware of the SANS Institute annual Top 20 Security Risks publication, <http://www.sans.org/top20/>, which provides “a consensus list of vulnerabilities that require immediate remediation.” Evaluators should be aware of this list to ensure that technical testing accounts for the published risks. Likewise, Business Owners and Facilitators should be aware of this list to ensure that the scope prepared for any given assessment includes testing for the published risks.

APPENDIX E: TESTING TOOLS

DISCLAIMER: The inclusion of a link, or the explicit identification of a tool, does not constitute an endorsement of that tool on the part of CMS or any CMS employee or third-party Business Partner. CMS has neither evaluated the suitability nor performed a technical assessment for any of the tools identified through these links.

Many automated tools exist within the industry that may be suitable for a security assessment of CMS systems. Potential testing tools include port scanners, vulnerability scanners, password cracking utilities, file integrity checkers, virus detectors, war dialer and war driver utilities. The links provided in table are identified for information purposes only, and do not constitute a complete list of testing resources.

1. Basic Tools

The Evaluator, during the planning of an assessment, will be expected to prepare a list of tools that will be used during the assessment. The web sites identified in Table 2 contain listings of tools commonly used to facilitate security assessments of the infrastructure or an application.

Table 1: Sources for Testing Tools

| <i>DESCRIPTION</i> | <i>LINK</i> |
|--------------------------------------|---|
| Top 100 Network Security Tools | http://sectools.org/ |
| UNIX Host and Network Security Tools | http://csrc.nist.gov/tools/tools.htm |
| Open Source Security Mother Lode | http://www.networksecurityjournal.com/features/open-source-security-tools-applications-resources-041007/ |
| Microsoft Baseline Security Analyzer | http://www.microsoft.com/technet/security/tools/mbsahome.msp |

The prepared list of tools to be used during the assessment may be required by the Facilitator, the Business Owner or CMS Management to ensure that the assessment process does not expose CMS systems to additional risks to production operations. The Evaluator shall record the full list of tools used during the assessment in the final security assessment report as defined by the *CMS Reporting Standard for Information Security Assessments*.

2. Live Distributions

The Evaluator may use freely available “live” system distributions, which are focused on security assessments. The web sites identified in Table 2 provide distribution files, which may be downloaded by the Evaluator for use during an assessment.

Table 2: Testing Tools Source List

| <i>LIVE DISTRIBUTION</i> | <i>LINK</i> |
|---|---|
| F.I.R.E. (Linux) | http://fire.dmzs.com/ |
| Helix (Linux) | http://www.e-fense.com/helix/ |
| INSERT Rescue Security Toolkit (Linux) | http://www.inside-security.de/insert_en.html |
| Knoppix Security Tools Distribution (STD) (Linux) | http://s-t-d.org/download.html |
| L.A.S. Linux (Linux) | http://www.localareasecurity.com/download |
| nUbuntu (Linux) | http://www.nubuntu.org/downloads.php |
| Operator (Linux) | http://www.ussysadmin.com/operator/ |
| PHLAX (Linux) | http://public.planetmirror.com/pub/phlak/?fl=p |
| BackTrack (Linux) | http://www.remote-exploit.org/backtrack.html |
| Knoppix (Linux) | http://www.knopper.net/knoppix-mirrors/index-en.html |

If the Evaluator uses a live distribution, the Evaluator may be required to identify the distribution, and the assessment tools used from the distribution, in the final assessment report. Live distributions shall not be permitted to operate from CMS workstations without the approval of CMS Management.

3. Virtualization

The Evaluator may also use virtualization utilities, such as VMWare and Xen, to create environments on non-CMS equipment from which the Evaluator may launch automated testing tools. As virtualization tools may allow for the creation of multiple network connections, the Evaluator may be required by the Facilitator, the Business Owner or CMS Management to disclose the use of virtualization utilities and to limit the network traffic from the equipment used for testing.

APPENDIX F: SOCIAL ENGINEERING

In information security, social engineering is a term that describes a non-technical process to subvert physical and personnel security measures which rely heavily on human interaction and often involves tricking other people into breaking normal security procedures.

Methods of Social Engineering

A social engineer conducts what used to be called a "con game". For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem; social engineers often rely on the natural helpfulness of people as well as on their weaknesses. Appeal to vanity, appeal to authority, and old-fashioned eavesdropping are typical social engineering techniques.

Phone - The most prevalent type of social engineering attack is conducted by phone. A hacker will call up and imitate someone in a position of authority or relevance and gradually pull information out of the user.

Instant Messaging (IM)/Chat - Intruders are using automated tools to post messages to unsuspecting users of IM or chat services. These messages typically offer the opportunity to download software of some value to the user, including improved music downloads, anti-virus protection or pornography. Once the users download and execute the software, though, their system is co-opted by the attacker for use as an agent in a distributed Denial-of-Service (DDoS) network.

Here is an example of one such message: You are infected with a virus that lets hackers get into your machine and read url files, etc. I suggest you to download [malicious url] and clean your infected machine. Otherwise you will be banned from [network].

Dumpster Diving - Information can be collected through company dumpsters. The following items are potential security leaks in the trash: company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or log-on names and passwords, print-outs of source code, disks and tapes, company letterhead and memo forms, and outdated hardware.

Many sources provide a rich vein of information for the hacker. Phone books give the hackers names and numbers of people to target and impersonate. Organizational charts contain information about people who are in positions of authority within the organization. Memos provide small tidbits of useful information for creating authenticity. Policy manuals can demonstrate how a company's security measures may be subverted. Calendars can be leveraged in a timely attack orchestrated around vacations, holidays, meetings or any occasions offering would-be attackers the ability to impersonate or occupy vacant facilities. Systems manuals, sensitive data and other sources of technical information may give hackers the keys they need to

unlock the network. Finally, outdated hardware and retired media, particularly hard drives, can be restored to provide all sorts of useful information.

Impersonating an Employee - Impersonation generally means creating some sort of character and playing out the role. The simpler the role, the better. Sometimes this could mean just calling up, saying: “Hi, I’m Joe in IS and I need your password,” but that does not always work. Other times, the hacker will study a real individual in an organization and wait until that person is out of town to impersonate him over the phone. According to Bernz, a hacker who has written extensively on the subject, they use little boxes to disguise their voices and study speech patterns and organizational charts. This is the least likely type of impersonation attack because it takes the most preparation, but it does happen.

Some common roles that may be played in impersonation attacks include: A repair person, IT support, a manager, a trusted third party (for example, the President’s executive assistant who is calling to say that the President okayed her requesting certain information), or a fellow employee. In a huge company, this is not that hard to accomplish. There is no way to know everyone - IDs can be faked. Most of these roles fall under the category of someone with authority, which leads us to ingratiation. Most employees want to impress the boss, so they will go out of their way to provide required information to anyone in power.

E-mail / Virus - E-mail can also be used for more direct means of gaining access to a system. For instance, e-mail attachments sent from someone of authenticity can carry viruses, worms and Trojan horses. A good example of this was an AOL hack, documented by VIGILANTE: “In that case, the hacker called AOL’s tech support and spoke with the support person for an hour. During the conversation, the hacker mentioned that his car was for sale cheaply. The tech supporter was interested, so the hacker sent an e-mail attachment ‘with a picture of the car’. Instead of a car photo, the e-mail executed a back-door exploit that opened a connection out from AOL through the firewall.”

On-Line - The Internet is fertile ground for social engineers looking to harvest passwords. The primary weakness is that many users often repeat the use of one simple password on every account: Yahoo, Travelocity, Gap.com, etc. Typically, once a hacker has one password, he or she will attempt to gain access to multiple accounts. One way in which hackers have been known to obtain this kind of password is through an on-line form: they can send out some sort of sweepstakes information and ask the user to put in a name (including e-mail address – that way, he or she might get that person’s corporate account password as well) and password. These forms can be sent by e-mail or through US Mail. US Mail provides a better appearance that the sweepstakes might be a legitimate enterprise.

Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Frequently, social engineers will memorize access codes by looking over someone's shoulder (shoulder surfing), or take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed.

Security experts propose that as our culture becomes more dependent on information, social engineering will remain the greatest threat to any security system.¹

Digital - Social engineering is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. It is used to test the human element and user awareness of security. It can reveal weaknesses in user behavior, such as failing to follow standard procedures. Social engineering can be performed through many means, including analog and digital (e.g., e-mail, instant messaging). One form of digital social engineering is known as *phishing*, where attackers attempt to steal information such as credit card numbers, social security numbers, user IDs, and passwords. Phishing uses authentic-looking e-mails to request information or direct users to a fake web-site to collect information. Other examples of digital social engineering are creating fraudulent e-mails and sending fake attachments that could mimic worm activity.

Analog - Another means of social engineering is analog (e.g., Conversation, executed in person or over the phone). Security testers using analog social engineering as part of a penetration test typically follow one or more standard procedures. In one procedure, the penetration tester poses as a user experiencing difficulty and calls the organization's help desk to gain information on the target network or host, obtain a log-on ID and credentials, or get a password reset. The second procedure involves posing as the Help Desk and calling a user to get the user to provide user IDs and passwords. Analog social engineering is also often used to gain physical access to an organization. Testers may pose as maintenance technicians, cleaning crew, high profile visitors, etc., to gain access to buildings or secured areas. Testers typically dress in disguise (for example, in maintenance uniforms) and may also have fake badges and identification.

A few methods for analog social engineering include target overload: Present the individual with so many decisions to make that they start to default to simple responses on those that seem innocuous. This is well presented by the movie "Sneakers" when Robert Redford's character had to get into a building, and his team overloads the guard, who in desperation just buzzes Redford into the building.

The second is fascination. A staged 'play' that is interesting to the target will, at worst, totally engross the target individual, and at best, distract them from their job. In fact, the methods and techniques are as varied as there are individuals on the planet. What they have in common is the desire to have someone behave in a manner that is counter to security. "Those who have the responsibility to protect security should be taught that it is far safer to maintain the safety of the security than to please or give in to someone who wants us to compromise it."²

Realistically, the human element is often the weakest component of an environment. As such, social engineering testing skills include persuasion, a high likeability factor, and the ability to appeal to a user's sympathetic side. Social engineering may be used to target specific individuals

¹ State of Wisconsin Department of Administration, Division of Enterprise Technology. Security <http://itsecurity.wi.gov/category.asp?linkcatid=1332&linkid=1188&locid=89>

² Kabay, M. E., "Social engineering in penetration testing: Overload and fascination" Security Strategies Alert Newsletter. <http://www.networkworld.com/newsletters/sec/2007/1112sec1.html>

or groups in the organization or may have a broad target set. Specific targets may be identified when the organization knows of an existing threat or feels that the loss of information from a person or specific group of persons could have a significant impact on the organization. Individual targeting can lead to embarrassment for those individuals, if the test team successfully elicits information or gains access. It is important that the results of social engineering are used for improving the security of the organization and not to single out individuals. Testers should produce a detailed final report that identifies both the successful and unsuccessful tactics used. This level of detail assists organizations in tailoring their security awareness training programs.³ Social Engineering, often referred to as “people hacking,” is an outside hacker’s use of psychological tricks on legitimate users of a computer system to gain information (e.g., usernames, passwords, personal identification numbers (PINS), credit card numbers and expiration dates) needed to gain access to their systems.⁴

Additional Information:

Miller, Darren. “Social Engineering: You Have Been A Victim.” WindowsSecurity.com. Jul 13, 2005. <http://www.defendingthenet.com/NewsLetters/SocialEngineering.htm>

³ Technical Guide to Information Security Testing (Draft). NIST 800-115. November 2007.

⁴FCC Computer Security Notice: Security Engineering. December 2002.
<http://csrc.nist.gov/groups/SMA/fasp/documents/security-ate/December-2002-2.pdf>

APPENDIX G: RESOURCES & REFERENCES

- E-Government Act of 2002, PL 107-347
- Government Accountability Office (GAO), *Federal Information Systems Audit Manual (FISCAM)*, GAO/AIMD-12.19.6, January 1999
- GAO, *Government Auditing Standards*, GAO-03-673G, June 2003
- Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003
- OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2007
- OMB, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-07-09, July 2007
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-42, *Guideline on Network Security Testing*, October 2003
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, Final Public Draft
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, Revision 2, Final Public Draft
- NIST SP 800-115, *Technical Guide to Information Security Testing*, Draft
- NIST Federal Information Processing Standards (FIPS) 191, *Guideline for the Analysis of Local Area Network Security*
- NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-63, *Electronic Authentication Guideline*, Version 1.0.1
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*
- NIST Interagency Report (IR) 7328, *Security Assessment Provider Requirements and Customer Responsibilities*, Initial Public Draft
- NIST IR 7358, *Program Review for Information Security Management Assistance (PRISMA)*
- Department of Health and Human Services (DHHS), *HHS Personnel Security/Suitability Handbook*, SDD/ASMB 1/98
- Centers for Medicare & Medicaid Services (CMS) *Information Security” Virtual” Handbook* (<http://www.cms.hhs.gov/InformationSecurity>)
- *Common Criteria for Information Technology Security Evaluation*, version 3.1, Revision 2, September 2007
- *Common Methodology for Information Technology Security Evaluation*, version 3.1, Revision 2, September 2007
- Carnegie Mellon Software Engineering Institute, *Introduction to the OCTAVE® Approach*, August 2003

APPENDIX H: ACRONYMS

| | |
|--------|---|
| AC | Access Control |
| ARS | Acceptable Risk Safeguards |
| ASP | Active Server Page |
| AT | Awareness and Training |
| C&A | Certification & Accreditation |
| CAP | Corrective Action Plan |
| CGI | Common Gateway Interface |
| CIA | Confidentiality Integrity and Availability |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CISS | CMS Integrated Security Suite |
| CMS | Centers for Medicare and Medicaid Services |
| CMSR | CMS Minimum Security Requirements |
| CPU | Central Processing Unit |
| DdoS | Distributed Denial-of-Service |
| DHHS | Department of Health and Human Services |
| DUA | Data Use Agreement |
| EASG | Enterprise Architecture and Strategy Group |
| EDI | Electronic Data Interchange |
| FA | FISMA Security Control Assessment |
| FIPS | Federal Information Processing Standards |
| FISCAM | Federal Information System Controls Audit Manual |
| FISMA | Federal Information Security Management Act |
| GAO | Government Accountability Office |
| GSS | General Support System |
| HIPAA | Health Insurance Portability and Accountability Act |
| HTTP | Hypertext Transfer Protocol |
| IA | Identification and Authentication |
| ICMP | Internet Control Message Protocol |
| IDS | Intrusion Detection System |
| IM | Instant Messaging |
| IR | Interagency Report |
| IRM | Information Resource Management |
| IRS | Internal Revenue Service |
| IS | Information Security |
| ISA | Interconnection Security Agreement |
| ISSO | Information System Security Officer |
| MA | Maintenance |
| MA | Major Application |
| MMA | Medicare Modernization Act |
| MOU | Memorandum of Understanding |
| NDA | Non-Disclosure Agreement |

| | |
|-------|--|
| NIST | National Institute of Standards and Technology |
| OAGM | Office of Acquisition and Grants Management |
| OIG | Office of Inspector General |
| OIS | Office of Information Services |
| OMB | Office of Management and Budget |
| OOM | Office of Operations Management |
| OS | Operating System |
| PIN | Personal Identification Number |
| PISP | Policy for the Information Security Program |
| POA&M | Plan of Action & Milestones |
| RA | Risk Assessment |
| RRT | Role Related Tasks |
| RoE | Rules of Engagement |
| SCT | Security Control Testing |
| SDLC | System Development Life Cycle |
| SEMG | Security and Emergency Management Group |
| SP | Special Publication |
| SQL | Structured Query Language |
| SSO | System Security Officer |
| SSP | System Security Plan |
| ST&E | Security Test & Evaluation |
| URL | Uniform Resource Locator |
| XSS | Cross-Site Scripting |

End of Document