

Office of Information Technology

Information Security & Privacy Group

Centers for Medicare & Medicaid Services

Security Assessment Plan

Template

**Version 3.0**

**January 9, 2019**

Table of Contents

[1. Introduction 2](#_Toc486240701)

[1.1 Purpose 2](#_Toc486240702)

[1.2 Security Control Assessment Background 2](#_Toc486240703)

[1.3 Assessment Process and Methodology 3](#_Toc486240704)

[1.3.1 Phase 1: Planning 3](#_Toc486240705)

[1.3.2 Phase 2: Assessment 3](#_Toc486240706)

[1.3.3 Phase 3: Reporting 4](#_Toc486240707)

[2. Planning 5](#_Toc486240708)

[2.1 Background 5](#_Toc486240709)

[2.2 Assessment Scope 5](#_Toc486240710)

[2.3 Assessment Assumptions/Limitations 6](#_Toc486240711)

[2.4 Data Use Agreement 7](#_Toc486240712)

[2.5 Roles and Responsibilities 7](#_Toc486240713)

[2.5.1 Business Owner 7](#_Toc486240714)

[2.5.2 CMS Facilitator 7](#_Toc486240715)

[2.5.3 CMS Government Task Lead 8](#_Toc486240716)

[2.5.4 Information System Security Officer or System Security Officer 8](#_Toc486240717)

[2.5.5 Lead Evaluator 8](#_Toc486240718)

[2.5.6 Privacy Officer 9](#_Toc486240719)

[2.5.7 Program Manager 9](#_Toc486240720)

[2.5.8 System Owner 9](#_Toc486240721)

[2.6 Assessment Responsibility Assignment 9](#_Toc486240722)

[3. Assessment 11](#_Toc486240723)

[3.1 Information Collection 11](#_Toc486240724)

[3.1.1 CMS FISMA Controls Tracking System (CFACTS) 11](#_Toc486240725)

[3.1.2 Documentation Requirements 11](#_Toc486240726)

[3.2 Enumeration 12](#_Toc486240727)

[3.2.1 Documentation Review 12](#_Toc486240728)

[3.3 Testing and Review 13](#_Toc486240729)

[3.3.1 Interviews 13](#_Toc486240730)

[3.3.2 Observances 13](#_Toc486240731)

[4. Reporting 14](#_Toc486240732)

[4.1 Security Control Assessment Findings Spreadsheet 14](#_Toc486240733)

[4.1.1 Row Number 16](#_Toc486240734)

[4.1.2 Weakness 16](#_Toc486240735)

[4.1.3 Risk Level 16](#_Toc486240736)

[4.1.4 CMSR Security Control Family and Reference 16](#_Toc486240737)

[4.1.5 Affected Systems 16](#_Toc486240738)

[4.1.6 Ease-of-Fix 17](#_Toc486240739)

[4.1.7 Estimated Work Effort 17](#_Toc486240740)

[4.1.8 Finding 17](#_Toc486240741)

[4.1.9 Failed Test Description 18](#_Toc486240742)

[4.1.10 Actual Test Results 18](#_Toc486240743)

[4.1.11 Recommended Corrective Actions 18](#_Toc486240744)

[4.1.12 Status 18](#_Toc486240745)

[4.2 Reassignment of Findings 18](#_Toc486240746)

[4.3 Test Reporting 19](#_Toc486240747)

[5. Logistics 20](#_Toc486240748)

[5.1 Points of Contact 20](#_Toc486240749)

[5.2 Assessment Schedule 20](#_Toc486240750)

[5.3 Assessment Estimated Timeline 21](#_Toc486240751)

List of Tables

[Table 1. Assessment Responsibilities 10](#_Toc486240752)

[Table 2. Tier 1 Documentation – Mandatory Pre-Assessment 12](#_Toc486240753)

[Table 3. Tier 2 Documentation - Required Two Weeks Prior to the Assessment 12](#_Toc486240754)

[Table 4. Findings Spreadsheet 15](#_Toc486240755)

[Table 5. Risk Definitions 16](#_Toc486240756)

[Table 6. Definition of Ease-of-Fix Rating 17](#_Toc486240757)

[Table 7. Definition of Estimated Work Effort Rating 17](#_Toc486240758)

[Table 8. <Assessor’s Name> Points of Contact 20](#_Toc486240759)

[Table 9. CMS Points of Contact 20](#_Toc486240760)

[Table 10. Vendor Points of Contact 20](#_Toc486240761)

[Table 11. Assessment Schedule 21](#_Toc486240762)

[Table 12. Estimated Timeline for Assessment Actions and Milestones 21](#_Toc486240763)

# Introduction

## Purpose

*<This document describes the Security Control Assessment (ASSESSMENT) methodology, schedule, and requirements that the <Assessor’s Name> will use to evaluate the system. The goal of the Security Assessment Plan is to clearly explain the information the <Assessor’s Name> expects to obtain prior to the assessment, the areas that will be examined, and the proposed scheduled activities the <Assessor’s Name> expects to perform during the assessment. This document is meant to be used by the Centers for Medicare & Medicaid Services (CMS), network engineers, and system administrators responsible for system operations.>*

## Security Assessment Background

*<Insert policies, regulations, guidelines, etc that inform the assessment>*

## Assessment Process and Methodology

*<This section outlines the assessment methodology to verify and validate that the management, operational, and technical controls are appropriately implemented.>*

### Phase 1: Planning

*<Phase 1, “Planning”, defines the assessment’s scope, identifies goals, sets boundaries, and identifies assessment activities.>*

### Phase 2: Assessment

*<Phase 2, “Assessment”, may have several steps depending on the assessment’s objectives, scope, and goals, as set forth in the Planning Phase. These steps can be grouped by the nature of the activities involved. These activity groups are as follows:*

***Information Collection****—thorough research that must be performed against the target system/application before any meaningful assessment can be conducted. Data gathered is analyzed as the assessment proceeds and when the assessment is complete.*

***Enumeration****—activities that provide specific information about assessment targets. This information is often collected using appropriate software tools.*

***Testing and Review****—activities that typically involve the automated testing of security vulnerabilities via software tools, manual analysis, and the evaluation of particular aspects of the organization’s security policies and practices by the <Assessor’s Name>. The <Assessor’s Name>’s goal is to apply experience and insight, in order to determine whether the system adequately implements security controls defined by CMS policies and standards.>*

### Phase 3: Reporting

*<Phase 3, “Reporting”, documents the soundness of the implemented security controls and consolidates all findings into the final output. This output includes reports that provide a summary of key findings and actionable recommendations, as well as provisions for all information derived from the assessment.*

*Depending on the results of these activities, it may be necessary to repeat appropriate phases. Throughout the entire process, the <Assessor’s Name> will keep all involved parties informed of the progress and findings, as well as provide briefings of findings to CMS. Evidence to support any weaknesses discovered will consist primarily of screen prints, script output, and session data. The <Assessor’s Name> will immediately notify CMS if significant or immediately exploitable vulnerabilities are discovered during the assessment.>*

# Planning

This section contains information describing the application and environment that will be assessed, the scope of the assessment, any limitations, and roles and responsibilities of staff who will participate in the assessment.

## Background

*<Provide system background information here.>*

## Assessment Scope

The <Assessor’s Name> is tasked with providing a comprehensive evaluation of *the <insert system information including security categorization.>*

Prior to the assessment, the <Assessor’s Name> will make several requests for documentation and other related artifacts such as to adequately prepare for the assessment. To adequately perform the assessment, the <Assessor’s Name> anticipates performing testing and interviews for *<insert amount of days for the assessment and the corresponding dates.>*

The assessment scope will include the following components:

* *<Provide list of components/controls>*

*<Provide additional scoping details as needed.>*

## Assessment Assumptions/Limitations

Assumptions

* *<Provide assumptions and limitations of the assessment as needed>*

## Data Use Agreement

The Data Use Agreement (DUA), form CMS-R-0235, must be executed prior to the disclosure of data from the CMS Systems of Records to ensure that the disclosure will comply with the requirements of the Privacy Act, Privacy Rule, and CMS data release policies. It must be completed prior to the release of, or access to, specified data files containing Protected Health Information (PHI) and individual identifiers. *<Insert the <Assessor’s Name>’s name and when they signed the data use agreement here.>*

## Roles and Responsibilities

To prepare for the assessment, the organization(s) and the <Assessor’s Name> will identify personnel associated with specific responsibilities. Individuals may have responsibilities that span multiple roles, or have knowledge pertaining to the implementation of more than one security control area. This section provides a description of the roles and responsibilities to assist the organization(s) and the *<Assessor’s Name>* in determining the appropriate personnel who should be available for the assessment.

### Business Owner

The Business Owner is responsible for the successful operation of the system and is ultimately accountable for system security. The Business Owner defines the system’s functional requirements, ensures that Security Accreditation (previously referred to as Certification and Accreditation [C&A]) activities are completed, maintains and reports on the Plan of Action & Milestones (POA&M), and ensures that resources necessary for a smooth assessment are made available to the <Assessor’s Name> (Assessment Contractor). During the assessment process, the Business Owner shall be available for planning sessions, interviews, system discussions, providing documentation, and providing assistance when necessary (access, contacts, decisions, etc.). In some cases, the Business Owner may be the System Owner.

### CMS Facilitator

The CMS Facilitator is a member of the CMS SCA Team staff responsible for scheduling and communicating information on all planning and coordinating meetings, as well as out-briefs associated with the assessment. The CMS Facilitator reserves work space for testing when the tests are conducted at CMS facilities. In addition, the CMS Facilitator coordinates the logistics between the CMS SCA Team and assessment stakeholders (application developers, maintainers, technical support, business owners, etc.). The CMS Facilitator is responsible for initiating application and system access for the test accounts used during the assessment. At the conclusion of the assessment, the CMS Facilitator accepts the Assessment Report, distributes the final report to assessment shareholders, and generates the cover letter associated with it.

### CMS Government Task Lead

The CMS Government Task Lead (GTL) is a CMS representative for the Application Developer/Maintainer, and is responsible for providing technical information to the <Assessor’s Name>. During the assessment process, the GTL shall be available for planning sessions, interview with their Application Developer/Maintainer, assisting the Application Developer during application discussions, providing assistance for using the application, and directing the Application Developer/Maintainer to remediate any weaknesses.

### Information System Security Officer or System Security Officer

The Information System Security Officer (ISSO), or System Security Officer (SSO), is responsible for ensuring that the management, operational, and technical controls to secure the system are in place and effective. The ISSO shall have knowledge of the following:

All controls implemented or planned for the system

Security audit controls and evidence that audit reviews occur

System Security Plan (SSP) and any authorized exceptions to security control implementations

The ISSO shall be responsible for all security aspects of the system from its inception, until disposal. During the assessment process, the ISSO plays an active role and partners with the CMS Facilitator to ensure a successful assessment. The ISSO shall be available for interview, provide or coordinate the timely delivery of all required assessment documentation; and coordinate and schedule interviews between the assessment team and assessment stakeholders. The ISSO is designated in writing, must be a CMS employee, and can be a System Developer/System Maintainer ISSO.

### Lead Evaluator

The Lead Evaluator is a member of the <Assessor’s Name> and responsible for understanding CMS policies, standards, procedures, system architecture and structures. The Lead Evaluator has limited activities within the assessment scope; reports all vulnerabilities that may impact the overall security posture of the system; refrains 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; and coordinates getting information, documentation and/or issues addressed between the <Assessor’s Name>, the CMS Facilitator, and the assessment Stakeholders. The Lead Evaluator must develop the *Assessment Plan;* modify the testing approach, when necessary according to the scope of the assessment; prepare the daily agenda, preliminary findings worksheets, and conduct the Assessment briefings; and prepare an Assessment Report (e.g., Findings Report) to communicate how the CMS business mission will be impacted if an identified vulnerability is exploited.

### Privacy Officer

The Privacy Officer provides development, guidance in the implementation and maintenance of the organizations information privacy policies and procedures, with which the system shall be in compliance. The Privacy Officer should perform periodic privacy risk assessments and conduct ongoing privacy control compliance monitoring and education across the enterprise. Other duties include overseeing the compliance monitoring of all employees, contractors, business associates, and other third parties. The Privacy Officer works in concert with the Information Security Officer to assure a mechanism to track access to Personally Identifiable Information (PII) and Protected Health Information (PHI) and reviews and receives appropriate audit activity, as well as assists the Security Officer with development and implementation of an information infrastructure that meets both privacy and security concerns. During the assessment process, the Privacy Officer shall be available for interview and provide documentation that falls under the Privacy Officer’s responsibility.

### Program Manager

The Program Manager shall have a high-level understanding of the assessed system, as well as the ability to describe organizational and system policies from an enterprise perspective, with which the system shall be in compliance. The Program Manager shall be familiar with; access controls (both physical and logical), contingency plans (i.e., alternate sites/storage, system restoration and reconstitution), user identification and authentication, system authorization to operate, incident response, resource planning, system and software acquisition, flaw remediation, and system interconnections and monitoring. During the assessment process, the Program Manager shall be available for interview and to provide documentation that falls under the Program Manager’s responsibility.

### System Owner

The System Owner is responsible for the successful operation of the system and accountable for system security. The System Owner is also responsible for executing crucial steps to implement management and operational controls, and to ensure that effective technical controls are implemented to protect the system and its data. The System Owner formally designates the ISSO. In conjunction with the Business Owner, the System Owner is responsible for ensuring that Security Accreditation activities are completed, and that the POA&M is maintained and reported. During the assessment process, the System Owner shall be available for interview and, with the assistance of the system’s support staff, ensure that all documentation required for the assessment is available to the assessment Evaluator. The System Owner may be the Business Owner.

## Assessment Responsibility Assignment

For this assessment, the <Assessor’s Name> and CMS have been associated with their specific roles and corresponding responsibilities. The Business Owner may delegate their responsibilities during the engagement, but the name of the delegated individual should be updated in Table 1, which provides details on the responsibilities for the assessment based on the identified roles and responsibilities provided in the preceding Section, “Roles and Responsibilities.”

Table 1. Assessment Responsibilities

| Name | Organization | Role |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Assessment

*<This section contains information describing the activities to be performed during the assessment for information collection, enumeration, testing and review.>*

## Information Collection

*<The <Assessor’s Name> will require access to documentation, operating system and network configuration data, and application information, etc in order to perform the assessment.>*

### CMS FISMA Controls Tracking System (CFACTS)

To ensure that the final security controls/findings worksheet can be properly loaded in to the CMS FISMA Controls Tracking System (CFACTS) at the end of the assessment, the <Assessor’s Name> must have the correct system name, as contained within CFACTS. This system name will be used to correctly populate the System Name field in the Final Management Worksheet delivered with the Final Report.

| CFACTS System Name |
| --- |
| * <Insert System Name>
 |

### Documentation Requirements

***The <Assessor’s Name> must obtain requested documentation and artifacts in a timely manner to avoid delays and improperly reporting findings.*** In order to effectively perform the assessment and have no delays in the assessment, the <Assessor’s Name> must receive the following information that pertains to the application and/or system under evaluation prior to arriving onsite. Failure to receive this information in a timely manner will impact the assessment’s quality and the <Assessor’s Name>’s ability to determine whether management, operational, and technical controls have been implemented properly, and potentially reporting false findings. ***To assist the <Assessor’s Name> in determining the completeness of this information and to serve as a checklist, CMS should use Table 2 and Table 3 as a prioritized request list, and include any comments that may be applicable (e.g., System Design Document [SSD] contains detailed network diagram, SSP contains hardware and software inventory, and configuration management document contains baseline configurations and approved exceptions to baselines).***

**Tier 1 Documentation - Mandatory Pre-Assessment:** *<Insert required documentation for pre-assessment.>*

Table 2. Tier 1 Documentation – Mandatory Pre-Assessment

| Document Element # | Document/Information Requested | ARSCMSR  | Comments |
| --- | --- | --- | --- |
|  |  |  |  |

**Tier 2 Documentation – Required *<Insert Agreed Amount of Time>* Prior to the Assessment:** The Assessor uses the time prior to the assessment to review documentation, system baseline configurations, or process evidence to prepare for deep-dive analysis into processes, procedures, or technical settings. To facilitate this, the documents in Table 3 must be provided *<Insert Agreed Amount of Time>* prior to the assessment. This will allow *<Assessor’s Name>* time to identify gaps in the documentation, such as references to supplemental documentation residing on SharePoint/network folders which was not originally provided. If the provided documentation does not fully meet the information request, *<Assessor’s Name>* will identify such gaps to CMS, so they can quickly retrieve and provide the additional information.

Table 3. Tier 2 Documentation - Required Two Weeks Prior to the Assessment

| Document Element # | Document/Information Requested | ARSCMSR | Comments |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

## Enumeration

The *<Assessor’s Name>* will use various methods and tools to enumerate the system and its security policies.

### Documentation Review

Prior to, and during the assessment, the <Assessor’s Name> will review documents provided by CMS. The review will assess whether appropriate management and operational controls have been implemented. However, it will also be used to augment technical controls. For example, if the ARS CMSR stipulates that the password length for the information system is required to be eight characters, and the SSP documents that the length of passwords is eight characters, the technical assessment will confirm whether passwords are configured to be eight characters in length. As a part of the assessment and when feasible, the *<Assessor’s Name>* will evaluate the adequacy and completeness of the SSP in accordance with CMS guidelines and provide feedback. In general, the *<Assessor’s Name>* will review, but not be limited to, the following sample set of documentation: SSP. For the complete documentation list, refer to Section 3.1.2. During the assessment, the *<Assessor’s Name>* will provide written evaluations of the ISRA, SSP, and CP, and use these evaluation documents as a basis for interview, discussion, and clarification.

## Testing and Review

*<The <Assessor’s Name> will perform activities that typically involve both the automated testing of security vulnerabilities via software tools, manual analysis, and the evaluation of particular aspects of the organization’s security policies and practices.*

*<Assessor’s Name> will perform the following assessment activities:*

*Conduct interviews with key staff to examine management, operational, and technical controls*

*Examine documentation to ensure adherence to CMS policies and standards*

*Collect artifacts/evidence that demonstrate the CMS security controls are operating as designed>*

### Interviews

Interviews will focus on a review of the management, operational, and technical controls associated with the CMSR, CMS TRA security policies, procedures, and standards. Interviews will also help gain a better understanding of the system environment’s security posture and will supplement findings identified during the technical testing. When available and applicable, electronic copies of additional written documentation will be collected for review. Subject Matter Experts (SME) in the following areas will be interviewed:

### Observances

During the course of the assessment, the <Assessor’s Name> will also scrutinize personnel and the physical environment, as applicable, to determine if security policies and procedures are being followed. Examples of areas that may be included are:

# Reporting

This section outlines how the <Assessor’s Name> will report vulnerabilities during the assessment.

## Security Control Assessment Findings Spreadsheet

The assessment findings spreadsheet (Table 4) is a running tabulation of findings identified during the assessment that is reviewed during Daily Out-Briefs (DOBs). Findings are broken out by day and then sorted according to risk level. For updates to a previous day’s findings, the updated cell is highlighted in yellow. Although high and moderate risk-level findings are discussed during the DOBs, questions pertaining to low risk-level findings may be raised for clarification. Further details about the spreadsheet columns are listed in the following sections.

Table 4. Findings Spreadsheet

*<Insert screenshot of Findings Spreadsheet as needed>*

### Row Number

Each vulnerability has a row number included to provide easy reference when the spreadsheet is printed and reviewed during DOBs. This row number is also included in the test reports for easy cross reference.

### Weakness

A brief description of the security vulnerability is described in the Weakness column.

### Risk Level

Each finding is categorized as a business risk, and assigned a risk level rating described as high-, moderate-, or low-risk. The rating is, in actuality, an assessment of the priority with which each vulnerability should be addressed. Based on CMS’ current implementation of the underlying technology and the assessment guidelines contained with the *CMS Reporting Procedure for Information System (IS) Assessments* document,[[1]](#footnote-1) the <Assessor’s Name> will assign these values to each Business Risk. The risk ratings are described in Table 5.

Table 5. Risk Definitions

| Rating | Definition of Risk Rating |
| --- | --- |
| * High Risk
 | * Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS business processes. Significant political, financial, and legal damage is likely to result
 |
| * Moderate Risk
 | * Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS
 |
| * Low Risk
 | * Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment
 |

### CMSR Security Control Family and Reference

The CMSR security control family, and control number that is affected by the vulnerability, is identified in the CMSR Security Control Family and the Reference columns.

### Affected Systems

The systems, (URLs, IP addresses, etc.), which are affected by the weakness, are identified in the Affected Systems column.

### Ease-of-Fix

Each finding is assigned an Ease-of-Fix rating described as Easy, Moderately Difficult, or Very Difficult. The ease with which the Business Risk can be reduced or eliminated is described using the guidelines in Table 6.

Table 6. Definition of Ease-of-Fix Rating

| Rating | Definition of Ease-of-Fix Rating |
| --- | --- |
| * Easy
 | * The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system, or data
 |
| * Moderately Difficult
 | * Remediation efforts will likely cause a noticeable service disruption
* A vendor patch or major configuration change may be required to close the vulnerability
* An upgrade to a different version of the software may be required to address the impact severity
* The system may require a reconfiguration to mitigate the threat exposure
* Corrective action may require construction or significant alterations to the manner in which business is undertaken
 |
| * Very Difficult
 | * The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling
* An obscure, hard-to-find vendor patch may be required to close the vulnerability
* Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity
* Corrective action requires major construction or redesign of an entire business process
 |

### Estimated Work Effort

Each finding has been assigned an Estimated Work Effort rating described as Minimal, Moderate, or Substantial. The estimated time commitment required for CMS or contractor personnel to implement a fix for the Business Risk is categorized in Table 7.

Table 7. Definition of Estimated Work Effort Rating

| Rating | Definition of Estimated Work Effort Rating |
| --- | --- |
| * Minimal
 | * A limited investment of time (i.e., roughly three days or less) is required of a single individual to complete the corrective action(s)
 |
| * Moderate
 | * A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions
 |
| * Substantial
 | * A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units
 |

### Finding

A detailed description of how the finding did not meet the test description. This provides information on how the actual results fail to meet the security requirement, as noted in the CMS security policy, CMS security requirements, CMS guidance or industry best practices published by the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), Center for Internet Security (CIS), or database vendors. The finding should have the paragraph from the original report and the date of the final report included in the description as the first line for easy reference in the POA&Ms.

### Failed Test Description

The expected results that the finding did not meet are documented. This description provides the specific information from the CMS security policy, requirements, guidance, test objective or published industry best practices.

### Actual Test Results

This provides specific information on the observed failure of the test objective, policy or guidance.

### Recommended Corrective Actions

The recommended actions to resolve the vulnerability are explained in the Recommended Corrective Actions column.

### Status

The Status column provides status information, such as when the vulnerability was identified or resolved.

## Reassignment of Findings

If during the assessment testing period, a finding is determined to be outside the scope of the system or the responsibility of the CMS System Business Owner and ISSO, the finding will be reported, and steps should be taken to reassign the finding to the rightful owner. The CMS Assessment Facilitator will attempt to contact the rightful owner, provide them with the appropriate information, and invite them to the balance of the Assessment proceedings. During the Assessment week, the CMS facilitator may assist the CMS System Business Owner and ISSO to obtain the rightful owner’s concurrence and responsibility for the finding.

However, it is ultimately the responsibility of the CMS System Business Owner and ISSO to obtain concurrence of the potential finding from the rightful owner, and follow through with the necessary reassignment steps prior to the Draft Report Review.  If the finding has already been reported in CFACTS, the System Business Owner and ISSO must obtain the CFACTS identifier from the rightful owner, and the finding will be closed in the report noting the re-assignment and CFACTS information in the status field. If the ownership of the finding has not yet been successfully re-assigned by the time of the Draft Report Review, the report will be finalized with the finding assigned to the system. It is then the responsibility of the CMS System Business Owner and ISSO to address at a later time and update CFACTS accordingly with the proper information.

Once a finding is reassigned, it should be documented in the System’s Risk Assessment (ISRA). The CMS System Business Owner and ISSO should review periodically, as the finding may directly impact the system.

## Test Reporting

The <Assessor’s Name> will also conduct a final out-brief, if needed, after the assessment is completed. Typically, the <Assessor’s Name> does not have the opportunity to review all the documentation, configurations, and script outputs while onsite, and will need additional days to finish identifying potential vulnerabilities. If this is the case, CMS will schedule a final out-brief within one week after the assessment is completed.

The <Assessor’s Name> will discuss and review all informational evidence of remediated findings that is supplied by CMS. The *<Assessor’s Name>* will diligently respond to inquiries made by CMS concerning the validity of findings and acknowledge any areas of concern that may occur. The substance of evidence will contain any mitigation proof reflective of, and as close to, the source of the impacted system as possible. The manner of evidence exchange will be tracked and protected by the <Assessor’s Name> Lead, GTL, CMS Facilitator, and authorized Points of Contact (POC) for the system(s) tested. ***If CMS authorizes the submission of remediation evidence after the assessment dates, the focus should be on addressing High and Moderate risk findings. In order to promptly meet schedules, the <ASSESSOR’S NAME> requests that all evidence of remediated findings be submitted to <ASSESSOR’S NAME> by the due date established by CMS. See Table 12 for assessment related milestones.***

Approximately three weeks following the final out brief, the <Assessor’s Name> will provide a draft test report. The test report takes the vulnerabilities identified in the findings spreadsheet, and reformats and sorts the information to conform to CMS guidelines contained within the *CMS Reporting Procedure for IS Assessments* document. CMS will be provided approximately one week to review the test report. Following a draft test report review conference call that will be scheduled by CMS, the <Assessor’s Name> will generate a final test report and a data worksheet. The data worksheet will contain all findings not closed during the assessment or the remediation period following the assessment.

# Logistics

## Points of Contact

The <Assessor’s Name> POCs for the assessment are listed in Table 8.

Table 8. <Assessor’s Name> Points of Contact

| Name | Position | Phone Number | Email Address |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

During assessments, testing problems may be encountered outside normal working hours and require that staff need to be contacted. The CMS POCs for the ASSESSMENT are listed in Table 9.

Table 9. CMS Points of Contact

|  |  |  |  |
| --- | --- | --- | --- |
| * **Name**
 | * **Position**
 | * **Phone Number**
 | * **Email Address**
 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

The Vendor POCs for the assessment are listed in Table 10.

Table 10. Vendor Points of Contact

| Name | Position | Phone Number | Email Address |
| --- | --- | --- | --- |
| * *Additional contacts added here and subsequent lines*
 | * *Insert title*
 | * *contact number*
 | * *email address*
 |

## ASSESSMENT Schedule

CMS will need to be available to improve the assessment’s efficiency and accuracy. The interactions with the <Assessor’s Name> may include; technical consultation, supervised access to systems, networks, infrastructures, facilities, and monitoring assessment activities. The following calendar outlines anticipated staff requirements.

**All positions are expected to attend, or be available for, the daily out-briefs.**

Assessment schedule can be found in Table 11.

Table 11. <Assessor’s Name> Assessment Schedule

| **Day 1:** | **Day 2:** | **Day 3:** | **Day 4:** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

***Note that where appropriate, the Business Owner, ISSO, or CMS Facilitator will be responsible for scheduling teleconference bridges for ASSESSMENT interviews, as well as securing space for the <Assessor’s Name> to use during the ASSESSMENT.***

## Assessment Estimated Timeline

Table 12 describes the estimated timeline for assessment actions and milestones.

Table 12. Estimated Timeline for Assessment Actions and Milestones

| Action/Milestone | Description | Date(s) |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#

1. http://www.cms.hhs.gov/informationsecurity/downloads/Assessment\_Rpting\_Procedure.pdf. [↑](#footnote-ref-1)