



Centers for Medicare & Medicaid Services

Framework for the Independent Assessment of Security and Privacy Controls for Enhanced Direct Enrollment Entities

Final

Version 1.2

March 6, 2018

Record of Changes

Version	Date	Author / Owner	Description of Change	CR #
1.0	December 20, 2017	CMS	Initial draft, modified from CMS RMH Framework, with FedRAMP inclusions specifically tailored to Non-Exchange Entities	N/A
1.1	January 31, 2018	CMS	MITRE Peer Review	N/A
1.2	March 6, 2018	CMS	Incorporated CMS ISPG Feedback to include Configuration Management Plan	N/A

CR: Change Request

Table of Contents

1. Introduction	1
1.1 Requirements Background.....	1
1.2 Purpose.....	1
2. Assessment Independence	1
2.1 Independent Third-Party Assessor	1
3. Assessment Scope	2
3.1 Scope of the Independent Security and Privacy Control Assessment	2
3.2 Vulnerabilities and Testing Scenarios	2
3.3 Assessment of Critical Security Controls	3
4. Assessment Planning.....	3
5. Security and Privacy Control Assessment Methodology	4
5.1 Security and Privacy Control Technical Testing	4
5.2 Network and Component Scanning	5
5.3 Configuration Assessment	5
5.4 Documentation Review.....	5
5.5 Personnel Interviews.....	6
5.6 Penetration Testing	7
6. Security and Privacy Assessment Reporting.....	7
6.1 SAR Content	8

List of Tables

Table 1. Core Security and Privacy Documentation.....	6
---	---

1. Introduction

The Federally Facilitated Exchange (FFE) is the custodian of sensitive information, such as Personally Identifiable Information (PII) for millions of US citizens. Business partners, including Non-Exchange Entities (NEE) that process Exchange customer information, share the responsibility for ensuring the protection of this sensitive information. Through continuous monitoring and regular security and privacy control testing, NEEs demonstrate that they meet this responsibility. This *Framework for Independent Assessment of Security and Privacy Controls* (hereafter simply the “Framework”) provides an overview of the independent security and privacy assessment requirements and the associated Centers for Medicare & Medicaid Services (CMS) reporting process for NEEs associated with the FFE.

1.1 Requirements Background

The Security Assessment Control, CA-2, documented in the *Non-Exchange Entity (NEE) System Security and Privacy Plan (SSP)* requires assessment of all security and privacy controls attributable to a system or application before connecting to the CMS Data Services Hub (Hub) every year. Moreover, the NEE Independent Assessors control, CA-2(1), specifies that an independent third-party assessor (IA) conduct this assessment.

1.2 Purpose

This Framework is designed to accomplish the following objectives:

- Define assessment independence and the independent third-party assessor (Section 2)
- Provide assessment planning considerations (Section 3)
- Provide a basic security and privacy control assessment methodology (Section 4)
- Summarize security and privacy assessment reporting (Section 5)

This document is not intended to provide detailed assessment planning and performance guidance.

2. Assessment Independence

2.1 Independent Third-Party Assessor

The security control, CA-2(1), requires the employment of assessors or assessment teams to conduct security and privacy control assessments of the NEE’s system. An assessor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the system and the determination of security and privacy control effectiveness.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk* states:

Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision.

Experience and competencies are important factors in selecting an IA. It is strongly recommended that the NEE select an IA from the Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization (3PAO) list.¹

3. Assessment Scope

3.1 Scope of the Independent Security and Privacy Control Assessment

The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application or system. The independent SCA provides an understanding of the following:

- The application or system's compliance with CMS-specified NEE security and privacy control requirements;
- The underlying infrastructure's security posture;
- Any application and/or system security, data security, and privacy vulnerabilities to be remediated to improve the security and privacy posture; and
- NEE adherence to the NEE's security and privacy program, policies, and guidance.

3.2 Vulnerabilities and Testing Scenarios

Given the sensitivity of data processed in the Exchange and the high threat of the web environment, it is important to ensure that the security of web applications deployed by FFE partners meet the present day known security attack vectors and situations. The Open Web Application Security Project (OWASP)² keeps an up-to-date list that identifies such attacks and situations. In addition to the security and privacy controls, the independent SCA requires penetration tests to determine vulnerabilities associated with known attacks and situations obtained from the current OWASP Top 10 - *The Ten Most Critical Web Application Security Risks*. The assessment should adjust the SCA scope to address the current OWASP vulnerabilities. The NEE should regularly review the following list to determine the current vulnerabilities in the OWASP Top 10, including, but not limited to:

- SQL Injection
- Broken Authentication and Session Management
- Sensitive Data Exposure
- XML External Entity (XXE)

¹ Available at: <https://marketplace.fedramp.gov/#!/assessors?sort=assessorName>.

² https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

3.3 Assessment of Critical Security Controls

Test scenarios must adequately assess the implementation status of critical security controls identified by the Center for Internet Security (CIS).³ The testing scenario information is available for each CIS control at the CIS site. The main testing points identified by the CIS are incorporated into the SCA scope, corresponding test plan, and testing criteria.

4. Assessment Planning

The NEE is encouraged to develop an assessment strategy and procedure that provides a standardized approach for planning and resourcing the SCA of its applications, systems, and underlying components. The NEE is responsible for ensuring that each SCA has:

- Budget and assigned resources suitable for completing the assessment;
- Clear objectives and constraints;
- Well-defined roles and responsibilities; and
- Scheduling that includes defined events and deliverables.

During planning for the SCA, the NEE develops a scope statement that is dependent upon, but not limited to, the following factors:

- Application or system boundaries
- Known business and system risks associated with the application or system
- Dependence of the application or system on any hierarchical structure
- Current application or system development phase
- Documented security and privacy control requirements

The IA SCA contract statement of work should include providing support to clarify findings and make corrective action recommendations after the assessment. The contract should also specify that all IA contractor staff must execute Non-Disclosure Agreements (NDA) before accessing any information related to the security and privacy of the application or system. Requests to access information should only be considered based on a demonstration of a valid need to know, and not a position, title, level of investigation, or position sensitivity level.

³ CIS Top 20 Critical Controls, available at: <https://www.cisecurity.org/controls/>.

5. Security and Privacy Control Assessment Methodology

The SCA methodology described in this Framework originates from the standard CMS methodology used in the assessment of all CMS internal and business partner application or systems.

Assessment procedures for testing each security and privacy control should be consistent with the methodology documented in NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. The IA should prepare a detailed assessment plan using these security and privacy control assessment procedures, the main testing points for the CIS critical controls, and detailed directions for addressing the penetration testing procedures for the OWASP Top 10 vulnerabilities. The *Security and Privacy Assessment Test Plan* can be used or referenced to ensure that the assessment plan addresses the required elements. The IA should modify or supplement the procedures to evaluate the application's or system's vulnerability to different types of threats, including those from insiders, the Internet, or the network. The assessment methods include examination of documentation, logs and configurations, interviews of personnel, and testing of technical controls. Control assessment procedures and associated test results provide information to identify the following:

- Application or system vulnerabilities, the associated business and system risks, and potential impact
- Weaknesses in the configuration management process, such as weak system configuration settings that may compromise the confidentiality, integrity, and availability (CIA) of the system
- CMS and/or NEE policies not followed
- Major documentation omissions and/or discrepancies

5.1 Security and Privacy Control Technical Testing

To conduct security technical testing, the NEE grants IA staff user access to the application or system. The NEE system administrator establishes application-specific user accounts for the technical assessor that reflect the different user types and roles. Through this access and these accounts, the technical assessor can perform a thorough assessment of the application or system and test application and system security controls that might otherwise not be tested. The assessor should not be given a user account with a role that would allow access to PII in any application or database.

The technical assessor should attempt to expose vulnerabilities associated with gaining unauthorized access to the application or system resources by selecting and employing tools and techniques that simulate vulnerabilities, such as buffer overflows and password compromises. The technical assessor must use caution to ensure against any inadvertent alteration of important settings that may disable or degrade essential security or business functions. Because many automated testing utilities mimic signs of attack and/or exploit vulnerabilities, the technical assessor must identify in the IA assessment plan all proposed tools that pose a risk to the computing environment. Furthermore, any testing that could potentially expose PII must be performed under the direct supervision of an authorized individual who is responsible for the

data and can monitor the technical assessor's actions and take appropriate measures to protect any data that is vulnerable to exposure.

5.2 Network and Component Scanning

To gain an understanding of a network and component infrastructure security posture, the SCA includes network-based infrastructure scans, database scans, web application scans, and penetration tests for all in-scope components, applications, and systems. This provides a basis for determining the extent to which the security controls implemented within the network meet security control requirements. The results of these scans are evaluated in conjunction with the configuration assessment.

5.3 Configuration Assessment

The configuration assessment performed provides the assessor with another mechanism for determining if the NEE's security requirements are implemented correctly in the application, system, or system environmental components within the boundary of the application or system. The process for performing the configuration assessment requires the assessor to:

- Review the implemented configurations for each component against the NEE's security and privacy requirements;
- Review access to the system and databases for default user accounts;
- Test firewalls, routers, systems, and databases for default configurations and user accounts;
- Review firewall access control rules against the NEE's security requirements; and
- Determine consistency of system configuration with the NEE's documented configuration standards.

5.4 Documentation Review

The assessor must review all security and privacy documentation for completeness and accuracy, and to gain the necessary understanding to determine the security and privacy posture of the application or system. Through this process, the assessor develops insight into the documented security and privacy controls in place to effectively assess whether all controls are implemented as described. The documentation review augments all testing: it is an essential element for evaluating compliance of the documented controls versus the actual implementation as revealed during technical testing, scanning, configuration assessment, and personnel interviews.

For example, if the CMS-specified control stipulates that the password length for the system is required to be eight characters, the assessor must review the NEE's password policy or the SSP to verify the documented password length is eight characters. During the technical configuration assessment, the assessor confirms passwords are configured as stated in the NEE's documentation. Table 1 identifies examples of core security documentation for review.

Table 1. Core Security and Privacy Documentation

NEE Control Family	NEE Control Number	Document Name
Planning (PL)	PL-2: System Security and Privacy Plan (SSP)	System Security and Privacy Plan (SSP)
Configuration Management (CM)	CM-9: Configuration Management Plan	Configuration Management Plan
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing and Exercises	Contingency Plan Test Plan and Results
Incident Response (IR)	IR-8: Incident Response Plan	Incident Response Plan (IRP)
Incident Response (IR)	IR-3: Incident Response Testing and Exercises	IRP Test Plan
Awareness and Training (AT)	AT-3: Security Training	Security Awareness Training Plan
Awareness and Training (AT)	AT-4: Security Training	Training Records
Security and Assessment Authorization (CA)	CA-3: System Interconnections	Interconnection Security Agreements (ISA)
Risk Assessment (RA)	RA-3: Risk Assessment	Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	Privacy Impact Assessment or other privacy documents
Authority and Purpose (AP)	AP-2: Purpose Specification	Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PII and Privacy Act Statements
Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program	Governance documents and privacy policy
Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment	Documentation describing the organization's privacy risk assessment process, documentation of privacy risk assessments performed by the organization

5.5 Personnel Interviews

The assessor conducts personnel interviews to validate the implementation of security and privacy controls, that staff understand and follow documented control implementations, and that updated documentation is appropriately distributed to staff. The assessor interviews business, information technology, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. The assessor will customize interviews to focus on control assessment procedures applicable to individual roles and responsibilities and assure proper implementation and/or execution of security and privacy controls.

The SCA test plan identifies the designated NEE subject matter experts (SME) to interview. These SMEs should have specific knowledge of overall security and privacy requirements and a detailed understanding of the application or system operational functions. The NEE staff selected for conducting interviews may have the following roles:

- Business Owner(s)
- Application Developer
- Configuration Manager
- Contingency Planning Manager
- Database Administrator
- Data Center Manager
- Facilities Manager
- Firewall Administrator
- Human Resources Manager
- Information System Security Officer
- Privacy Program Manager
- Privacy Officer
- Media Custodian
- Network Administrator
- Program Manager
- System Administrators
- System Owner
- Training Manager

Although the initial identification of interviewees is determined when the IA assessment plan is prepared, additional staff may be identified for interviewing during the interview process.

5.6 Penetration Testing

At a minimum, penetration testing includes the tests found in subsection 2.2.1 (based on the OWASP Top 10. The *Security and Privacy Controls Assessment Test Plan* should properly document the tools, methods, and processes for penetration testing. The test plan should clearly account for and coordinate any special requirements or permissions for penetration testing during the SCA.

6. Security and Privacy Assessment Reporting

At the completion of the assessment, the assessor provides a Security and Privacy Assessment Report (SAR) to the Business Owner, who is then responsible for providing the report to CMS. The SAR structure and content provides the information noted in the next subsection and is consistent with the assessment objectives. The SAR allows the IA to communicate the assessment results to several audience levels, ranging from executives to technical staff.

6.1 SAR Content

The SAR content includes the following information (please refer to the SAR Template for additional details):

- System Overview
- Summary Report
- Detailed Findings Report
- Scan Results
- Infrastructure
 - Database
 - Web Applications
- Penetration Test Report
- Scan Results Summary

The SAR presents the results of all testing performed, including technical testing, scans, configuration assessment, documentation review, personnel interviews, and penetration testing. Results from multiple testing sources may be consolidated in one finding, if findings are closely related. The findings of the assessment should be annotated in detail with the remediation recommendations for the weaknesses and deficiencies found in the system security and privacy controls implementation. To reduce the risks posed to this important healthcare service and to protect the sensitive information of the citizens who use this service, the assessment team must assign business and system risk levels to each specific finding. The assignment of these risk levels should follow the methodology outlined in NIST SP 800-30, Appendices G, H, and I.⁴ When assigning risk levels, CMS requires only three levels of granularity:

- **High** – a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, and other organizations.
- **Moderate** – a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, and other organizations.
- **Low** – a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, and other organizations.

⁴ NIST 800-30, Appendices G, H, and I. Available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.