Centers for Medicare & Medicaid Services

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

Final

Version 2.0

March 8, 2019

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
2.0	March 8, 2019	CMS	Version 2.0 for release to Non-Exchange Entities	N/A

CR: Change Request

Table of Contents

List of Tables

1. Introduction

The Federally-facilitated Exchange (FFE) is the custodian of sensitive information, such as Personally Identifiable Information (PII) for millions of U.S. citizens. Business partners, including Non-Exchange Entities (NEE) that process Health Insurance Exchange (hereafter simply “the Exchange”) customer information, share the responsibility for ensuring the protection of this sensitive information. Enhanced Direct Enrollment (EDE) Entities are considered NEEs. Through continuous monitoring and regular security and privacy control testing, EDE Entities 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 EDE Entities associated with the FFE.

1.1 Requirements Background

The Security Assessment Control, CA-2, documented in the *Enhanced Direct Enrollment (EDE) Entity 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 EDE Security Control, CA-2(1), Independent Assessors Control, specifies that an independent third-party assessor (also referred to as the “Auditor”) conduct this assessment. EDE Entities must have a fully completed and implemented SSP before starting the security and privacy audit.

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); and
- Summarize security and privacy assessment reporting (Section 5).

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

2. Assessment Independence

2.1 Independent Third-Party Assessor (Auditor)

The Security Assessment Control, CA-2(1), requires the employment of Auditors or assessment teams to conduct security and privacy control assessments of the EDE Entity’s environment. The Auditor’s role is to provide an independent assessment of the compliance of the enhanced direct enrollment pathway and to maintain the integrity of the audit process. An Auditor 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. Upon submission of the audit, the Auditor will be required to attest to their independence and objectivity in completing the audit and that neither the EDE Entity nor the Auditor took any actions that might impair the objectivity of the findings in the audit.

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

> 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 Auditor. CMS requires that the EDE Entity's Auditor possess a combination of privacy and security experience and relevant auditing certifications. Examples of acceptable privacy and security experience include, but are not limited to:

- Federal Information Security Management Act (FISMA) experience;
- Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization;
- Statement on Standards for Attestation Engagements (SSAE) 16 experience;
- Reviewing compliance with NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; and
- Reviewing compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule standards.

Examples of relevant auditing certifications are:

- Certified Information Privacy Professional (CIPP);
- Certified Information Privacy Professional/Government (CIPP/G);
- Certified Information Systems Security Professional (CISSP);
- Fellow of Information Privacy (FIP);
- HealthCare Information Security and Privacy Practitioner (HCISPP);
- Certified Internal Auditor (CIA);
- Certification in Risk Management Assurance (CRMA);
- Certified Information Systems Auditor (CISA); or
- Certified Government Auditing Professional (CGAP).

CMS strongly recommends that the EDE Entity select an Auditor 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 independently conducted SCA provides an understanding of the following:

- The application or system's compliance with CMS-specified EDE Entity 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 EDE Entity's security and privacy posture; and
- The EDE Entity's adherence to its 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 critically important 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 mandated 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 EDE Entity 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);
- Broken Access Control;
- Security Misconfiguration;
- Cross-Site Scripting (XSS);
- Insecure Deserialization;

[1] Available at: https://marketplace.fedramp.gov/#/assessors?sort=assessorName.

[2] Available at: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

- Using Components with Known Vulnerabilities; and
- 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 Security and Privacy Controls Assessment Test Plan (SAP)[4], and testing criteria.

4. Assessment Planning

The EDE Entity 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 EDE Entity 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 EDE Entity develops a scope statement that is dependent on, 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; and
- Documented security and privacy control requirements.

The Auditor's SCA contract statement of work should include contractual requirements to provide support to clarify findings and make corrective action recommendations after the assessment. The contract terms should also specify that all Auditor 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/.

[4] The EDE SAP template is available on CMS zONE.

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 Auditor 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 EDE SAP can be used or referenced to ensure that the assessment plan addresses the required elements. The Auditor 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 should 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; and
- Major documentation omissions and/or discrepancies.

5.1 Security and Privacy Control Technical Testing

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

The Auditor 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 Auditor 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 Auditor must identify in the EDE SAP 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 Auditor'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 scope provides a basis for determining the extent to which the security controls implemented within the network meet security control requirements. The Auditor evaluates the results of these scans in conjunction with the configuration assessment.

5.3 Configuration Assessment

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

- Review the implemented configurations for each component against the EDE Entity'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 EDE Entity's security requirements; and
- Determine consistency of system configuration with the EDE Entity's documented configuration standards.

5.4 Documentation Review

The Auditor must review all security and privacy documentation for completeness and accuracy and gain the necessary understanding to determine the security and privacy posture of the application or system. Through this process, the Auditor 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 must be eight characters, the Auditor must review the EDE Entity's password policy or the SSP to verify compliance with this requirement. During the technical configuration assessment, the Auditor confirms passwords are configured as stated in the EDE Entity's documentation. Table 1 identifies examples of core security documentation for review.

Table 1. Core Security and Privacy Documentation

EDE Entity Control Family	EDE Entity 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 (CMP)
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing and Exercises	CP 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 (PIA) 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 Auditor conducts personnel interviews to validate the implementation of security and privacy controls, confirm that staff understand and follow documented control implementations, and verify the appropriate distribution of updated documentation to staff. The Auditor interviews business, information technology, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. The Auditor will customize interview questions to focus on control assessment procedures applicable to individual roles and responsibilities and assure that EDE Entity staff are properly implementing and/or executing security and privacy controls.

The SCA test plan identifies the designated EDE Entity 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 EDE Entity 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; and
- Training Manager.

Although the initial identification of interviewees is determined when the EDE SAP 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 3.2 (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 Auditor provides a Security and Privacy Assessment Report (SAR) to the Business Owner, who is then responsible for providing the report to CMS. The SAR’s structure and content (as described in the following subsection) must be consistent with the assessment objectives. The SAR allows the Auditor to communicate the assessment results to several audience levels, ranging from executives to technical staff.

The SAR is not a living document; findings should not be added and removed from the SAR unless CMS's initial review of the final draft discovers deficiencies or inaccuracies that should be addressed.

6.1 SAR Content

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

- System Overview;
- Executive Summary Report;
- Detailed Findings Report;
- Scan Results
  - Infrastructure Scan
  - Database Scan
  - Web Applications Scan;
- Penetration Test Report; and
- Penetration Test and 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.[5] 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.

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