DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Center for Consumer Information and Insurance Oversight
200 Independence Avenue SW
Washington, DC 20201

Date: **February 14, 2024**
From: **Center for Consumer Information and Insurance Oversight**
Title: **Health Insurance Exchange Guidelines**
Subject: **Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements**[1]

Table of Contents

I. Summary 2
II. Background 5
III. Information for Existing EDE Entities and Certain Prospective EDE Entities 7
IV. Enhanced Direct Enrollment Arrangements 13
V. Selection of an Auditor 25
VI. Business Audit Requirements and Scope 27
VII. Privacy and Security Audit Requirements and Scope 53
VIII. Required Auditor and EDE Entity Training 60
IX. DE/EDE Entity Program Management Environment (PME) Site for Document Submission 62
X. Approval Process and Audit Submission Window 62
XI. Processes for Changes to an Audited or Approved EDE Environment 71
XII. Resources 75
Appendix A. Privacy and Security Controls for Hybrid Non-issuer Upstream EDE Entities 79

[1] *The contents of this document do not have the force and effect of law and are not meant to bind the public in any way, unless specifically incorporated into a contract. This document is intended only to provide clarity to the public regarding existing requirements under the law.*

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense.

I. Summary

The Centers for Medicare & Medicaid Services (CMS) is continuing to implement Enhanced Direct Enrollment (EDE), an optional program allowing approved EDE Entities[2] (e.g., Qualified Health Plan [QHP] issuers and web-brokers[3] approved to participate in EDE) registered with or utilizing the Federally-facilitated Exchange (FFE, also known as the Marketplace) and State-based Exchanges on the Federal Platform (SBE-FPs), to host an application for Exchange[4] coverage on their own websites.[5] Participation in EDE requires integration with a suite of Exchange application programming interfaces (APIs). The APIs allow EDE Entities approved to participate in EDE to create, modify, submit, and retrieve Exchange data.

Based on the EDE implementation experience for the plan year (PY) 2024 open enrollment period (OEP), CMS is revising EDE operational and technical standards for the remainder of PY 2024 and PY 2025, including the PY 2025 OEP, hereinafter referred to as Year 7 of EDE, effective on the publication date of these Guidelines.

CMS offers an annual audit submission window when prospective primary EDE Entities[6] may submit audits to apply for EDE participation, and prospective phase change EDE Entities may submit audits to change end-state eligibility application phases. Prospective primary EDE Entities are entities that are seeking approval to use their EDE environments for the first time. Prospective phase change EDE Entities are primary EDE Entities already approved to use the EDE pathway that are seeking to implement a new eligibility application phase (see Section XI.A.ii, EDE Entity-initiated Phase Change Requests, for more information).

---

[2] References to "EDE Entity" or "EDE Entities" throughout these guidelines may apply to DE technology providers providing technology services on behalf of QHP issuers or web-brokers to enable their participation in EDE if those entities are developing and/or maintaining a QHP issuer's or web-broker's EDE technology platform. An "agent or broker DE technology provider," as currently defined in 45 C.F.R. § 155.20, means "a type of web-broker business entity that is not a licensed agent or broker under State law and has been engaged or created by, or is owned by an agent or broker, to provide technology services to facilitate participation in direct enrollment under §§ 155.220(c)(3) and 155.221."A "QHP issuer DE technology provider," as currently defined in 45 C.F.R. § 155.20, means "a business entity that provides technology services or provides access to an information technology platform to QHP issuers to facilitate participation in direct enrollment under §§ 155.221 or 156.1230, including a web-broker that provides services as a direct enrollment technology provider to QHP issuers. A QHP issuer direct enrollment technology provider that provides technology services or provides access to an information technology platform to a QHP issuer will be a downstream or delegated entity of the QHP issuer that participates or applies to participate as a direct enrollment entity."

[3] The term "web-broker," as currently defined in 45 C.F.R. § 155.20, means "an individual agent or broker, group of agents or brokers, or business entity registered with an Exchange under § 155.220(d)(1) that develops and hosts a non-Exchange website that interfaces with an Exchange to assist consumers with direct enrollment in QHPs offered through the Exchange as described in § 155.220(c)(3) or § 155.221. The term also includes an agent or broker direct enrollment technology provider."

[4] Exchange has the meaning set forth in 45 C.F.R. § 155.20. However, the EDE program does not extend to State-based Exchanges (SBEs) or Small Business Health Options Program (SHOP) Marketplaces. Therefore, as used in these Guidelines, the term "Exchange" does not include SBEs that do not rely on the Federal Platform or SHOP Marketplaces.

[5] The list of Entities Approved to Use EDE is available on the Direct Enrollment and Enhanced Direct Enrollment webpage at the following link: https://www.cms.gov/programs-and-initiatives/health-insurance-marketplaces/direct-enrollment-and-enhanced-direct-enrollment.

[6] Primary EDE Entities are described in more detail in Section IV.A, Providing an EDE Environment to Other Entities.

The audit submission window for prospective primary EDE Entities and prospective phase change EDE Entities interested in implementing EDE or changing phases during Year 7of EDE is from April 1, 2024 to July 1, 2024 at 3:00 AM ET. As detailed further in Section X.C, Audit Submission Completeness Review, CMS will conduct completeness reviews on all prospective primary EDE Entity and prospective phase change EDE Entity audits submitted within the applicable submission window; however, the Entity's opportunities to correct completeness deficiencies depends, in part, on when it submits its audit in the audit submission window. CMS will not review audits until the submission window begins. There is no guarantee that every prospective primary EDE Entity or prospective phase change EDE Entity that submits a complete audit within the submission window will receive approval prior to the PY 2025 OEP or during the 2024 calendar year. CMS strongly encourages EDE Entities to submit complete audits as early as possible within the audit submission window. Please review Section X.B, Audit Submission, for more detailed information on completeness reviews during the audit submission window. To aid in expediting the approval process, an upstream EDE Entity[7] should work with its primary EDE Entity to notify CMS of the proposed arrangement and submit the operational and oversight documentation to CMS for review.[8] Based on the documentation provided to CMS, CMS will determine if any additional audit requirements must be met prior to the upstream EDE Entity receiving approval. This approval will only occur with or after the primary EDE Entity's approval.

Developing and auditing an EDE environment may take considerable effort and time (e.g., it may take up to or more than a year). Once an Entity submits a complete audit, the approval process typically involves multiple resubmissions on behalf of the Entity. The need for resubmissions may stem from compliance findings in the audit submission and resubmissions, and issues and findings in the EDE environment and eligibility application. The number of resubmissions and back-and-forth communication also depends on how thoroughly and quickly Entities address issues and findings. Therefore, the EDE approval process typically takes many months after an audit submission has been deemed complete, and may take up to a year or more depending on the selected end-state phase, the quality of the build of the EDE environment, the quality of the audit and documentation submitted to CMS, and the quality and timeliness of resubmissions. Based on CMS's experience with prior audits, prospective EDE Entities that submit complete audits later in the audit submission window (i.e., mid-to-late May through June), depending on the quality of the submission and phase (among other factors), have a lower probability of being approved to go live before the OEP. No prospective EDE Entity will be approved unless and until the Entity meets all program requirements. CMS will not review audits—neither new submissions nor submissions deemed incomplete by CMS that are resubmitted and accompanied by additional documentation to remedy the initial finding of incompleteness—received after July 1, 2024 (at 3:00 AM ET). CMS will release future guidance about the next annual audit submission window.

[7] Upstream EDE Entities are described in more detail in Section IV.A, Providing an EDE Environment to Other Entities.

[8] Please refer to Sections IV.A, Providing an EDE Environment to Other Entities and XI.A, EDE Entity-initiated Change Requests, for more information.

A. Summary of Significant Changes

CMS is providing a brief summary of significant changes made in these guidelines. CMS does not intend for this summary to replace a thorough review of the EDE Guidelines in full.

1. As described in Section VI.A, CMS will no longer accept business audit submissions from primary EDE Entities intending to use eligibility application end-state Phase 1. Additionally, CMS is announcing limitations on primary EDE Entities implementing eligibility application end-state Phase 2 and a period to transition to eligibility application end-state Phase 3.
2. As described in Section VI, Exhibit 2, CMS has modified the requirements for consumer identity proofing in the Consumer pathway prior to calling the Person Search API.
3. As described in Section VII.A.i, Exhibit 7, CMS has modified the quarterly deadlines for certain privacy and security documentation requirements.

B. EDE Guidelines Quick Reference Guide

CMS is providing a quick reference guide for prospective and existing EDE Entities and their Auditors that identifies common scenarios and the accompanying commonly referenced sections. CMS does not intend for these quick references to replace a thorough review of the EDE Guidelines in full. CMS strongly encourages EDE Entities and their Auditors to review the entire document as it contains information on standards and requirements relevant to obtaining and maintaining approval to operate as an EDE Entity, including information on the third-party auditor operational readiness reviews. EDE Entities and their Auditors should also refer to the relevant statutes, regulations, and other interpretive materials for complete and current information on applicable requirements.

Scenario	Entity Type(s)	EDE Guidelines Section(s)
EDE Entities that intend to make a change to an audited or approved EDE Environment, including an application phase change	• Primary EDE Entity (prospective and existing) • Upstream EDE Entity (prospective and existing)	• XI.A, EDE Entity-initiated Change Requests
EDE Entities (e.g., issuers or web-brokers) that intend to use a primary EDE Entity's EDE Environment as an upstream EDE Entity	• Primary EDE Entity (prospective and existing) • Upstream EDE Entity (prospective and existing)	• IV.A, Providing an EDE Environment to Other Entities • XI.A, EDE Entity-initiated Change Requests
Agents or Brokers that intend to use a primary EDE Entity's pathway as a downstream agent or broker	• Primary EDE Entity (prospective and existing) • Agents or Brokers	• IV.B, Downstream Third-party Agent and Broker Arrangements • XI.A, EDE Entity-initiated Change Requests
EDE Entities that intend to hire an auditor to conduct an audit and need information to find a suitable auditor	• Primary EDE Entity (prospective and existing) • Upstream EDE Entities with audit requirements	• V, Selection of an Auditor
EDE Entities that intend to submit an audit during the audit submission window that need information on required pre-audit steps and best practices, as well as the audit completeness requirements	• Primary EDE Entity (prospective)	• VI.C.iii, Best Practices Prior to the Audit • VI.C, Application Technical Assistance • X.A, Pre-Audit Notification to CMS • X.C, Audit Submission Completeness Review

II. Background

CMS aims to foster a better consumer experience with the EDE pathway. EDE Entities and CMS accomplish this objective by providing consumers in FFE and SBE-FP states with additional methods to shop and apply for individual market Exchange coverage and by allowing consumers to work with an EDE Entity to enroll in an individual market QHP through the Exchange without requiring consumers to log on to HealthCare.gov. Using the API suite, EDE Entities can innovate and implement improvements to the application and enrollment process. The EDE API suite provides an EDE Entity with the data and tools necessary to fully manage customer relationships, including the ability to update applications and enrollments when necessary, as well as to assist consumers with various post-enrollment activities such as remedying open consumer Data Matching Issues (DMIs)/Special Enrollment Period Verification Issues (SVIs) and payment issues. CMS anticipates the EDE pathway will result in increased effectuation rates.

These Guidelines define operational and technical details related to the EDE program audit requirements, and discuss requirements and considerations for prospective primary and phase change EDE Entities' selection of an Auditor, as well as the scope of the operational readiness review (ORR) prospective EDE Entities must undertake to demonstrate they are prepared to provide EDE services through use of the EDE pathway.

The ORR process and CMS approval are necessary because of the effects an EDE Entity's processes may have on the HealthCare.gov information technology (IT) platform and consumers' eligibility applications.

When using the EDE pathway, a primary EDE Entity provides a full application,[9] enrollment, and post-enrollment support experience on its website(s), and must implement the full EDE API suite of required services, regardless of the EDE Entity's chosen application phase.[10] For Year 7 of EDE, this suite of required services includes the following APIs: Store ID Proofing, Person Search, Create App, Create App from Prior Year App, Store Permission, Revoke Permission, Get App, Add Member, Remove Member, Update App, Submit App, Get Data Matching Issue (DMI), Get Special Enrollment Period Verification Issue (SVI), Metadata Search, Notice Retrieval, Submit Enrollment, Document Upload, System and State Reference Data, Get Enrollment, Payment Redirect[11], Update Policy, and Events Based Processing. This list excludes optional APIs[12].

The EDE Entity is able to transfer information directly between its application and the Exchange by integrating its unique user interface (UI) with the EDE API suite. The Exchange continues to be responsible for determining each consumer's eligibility and issuing Eligibility Determination Notices (EDNs).

---

[9] An EDE Entity's EDE environment and application may not support all applicant eligibility scenarios or application changes depending on the EDE Entity's chosen phase, as described below in Section VI.A, Application Phase Options.

[10] Please refer to Section VI.A, Application Phase Options

[11] For information on exceptions to the requirement for EDE Entities to integrate with the Payment Redirect API, see Section 13.3, Payment Redirect Integration Requirements, of the EDE API Companion Guide, available at the following link: https://zone.cms.gov/document/api-information.

[12] For more information on APIs, see the Application Program Interface (API) Information Section of CMS zONE, available at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment.

To pursue EDE, prospective primary EDE Entities must build their EDE environments and submit audits consisting of two parts, a Business Requirements Audit and a Privacy and Security Audit, within the submission window established by CMS.[13] To pursue an eligibility application phase change, prospective phase change EDE Entities must update their EDE applications in one or more separate environments—to maintain at least one testing environment that reflects their production EDE environments—and submit EDE Entity-initiated Change Requests, consistent with Section XI.A, EDE Entity-initiated Change Requests, prior to conducting a phase change business requirements audit. Each prospective primary EDE Entity and prospective phase change EDE Entity must engage one or more independent Auditors to perform these audits and certify that the Entity's website(s) and operations comply with applicable program requirements prior to CMS approving the Entity to use the EDE pathway or to change application phases. For prospective primary EDE Entities, the applicable program requirements are listed in Exhibit 2 (Business Requirements) and Exhibit 6 (Privacy and Security Requirements) of these Guidelines. For prospective phase change EDE Entities, the applicable program requirements are listed in Exhibit 11 (Business Audit Phase Change Requirements) of these Guidelines. In addition, there may be audit submission requirements for certain upstream EDE Entities as described in Sections IV.A.iv, Privacy and Security Audit Requirements for Hybrid Non-issuer Upstream EDE Entities, and IV.A.v, Privacy and Security Audit Requirements for Hybrid Issuer Upstream EDE Entities Implementing Single Sign-On.

CMS will also conduct ongoing oversight of each EDE Entity in a manner generally consistent with that provided in previous plan years, including regular oversight of the Entity's EDE end-user experience in its production and testing environments. Entities must ensure that testing environments used for CMS testing are secured with user access credentials. Each prospective and approved primary EDE Entity must maintain a testing environment that accurately represents the EDE Entity's EDE production environment and integration with the EDE pathway, including functional use of all EDE APIs. The environment must reflect the EDE end-user experience.[14] Changes deployed to the production environment must be concurrently deployed to the test environment mirroring production. This may require an EDE Entity to develop a third environment for developing and testing new, unapproved changes. An EDE Entity must not submit test data to FFE Production Environments.

A. Authority

Pursuant to 45 C.F.R. §§ 155.220(c)(3)(ii), 155.221, 155.260, 156.265(b), and 156.1230, an EDE Entity must comply with applicable requirements, including demonstrating operational readiness to use the EDE pathway. Pursuant to 45 C.F.R. § 155.221(e), the Department of Health & Human Services (HHS) may immediately suspend the EDE Entity's ability to transact information with the Exchange if HHS discovers circumstances that pose unacceptable risk to

[13] For more information on the audit requirements for prospective primary EDE Entities, see the discussion of the Business Requirements Audit and Privacy and Security Audit Requirements in Sections VI, Business Audit Requirements and Scope; VII, Privacy and Security Audit Requirements and Scope; and XI.A, EDE Entity-initiated Change Requests. Additionally, there are separate audit requirements for some entities that are not primary EDE Entities (e.g., Hybrid Non-issuer Upstream EDE Entities). For more information, please refer to Section IV.A, Providing an EDE Environment to Other Entities, and its subsections. Also see https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/EDE-2019-Non-Issuer-FAQ.pdf.

[14] Please refer to Section IV.A, Providing an EDE Environment to Other Entities, for more information.

the accuracy of the Exchange's eligibility determinations, Exchange operations, or Exchange information technology systems until the incident or breach is remedied or sufficiently mitigated to HHS' satisfaction.[15]

Pursuant to 45 C.F.R. § 155.221(f)-(h), a prospective primary EDE Entity and prospective phase change EDE Entity must retain one or more independent third-party Auditors to perform an ORR to validate compliance with EDE program requirements (see Section V, Selection of an Auditor, for details pertaining to the selection of an Auditor). The prospective primary EDE Entity will identify the Auditor(s) it has selected for verifying program compliance in each of the two agreements the Entity must sign with CMS: an EDE Business Agreement, which sets forth consumer communication and operational requirements, and an Interconnection Security Agreement (ISA), which sets forth privacy and security requirements.[16] In addition, a prospective phase change EDE Entity or an existing primary EDE Entity that wants to add functionality or systems or otherwise make changes to its EDE environment must follow the processes for EDE Entity-initiated changes as detailed in Section XI, Processes for Changes to an Audited or Approved EDE Environment.

A primary EDE Entity may provide its approved EDE environment to upstream EDE Entities for use. Upstream EDE Entities that want to add functionality or systems or otherwise make changes to their respective primary EDE Entity's approved EDE environment beyond minor branding changes or QHP display changes[17] may also be required to complete an ORR that includes a privacy and security audit conducted by an independent, third-party Auditor. Please review Section IV.A, Providing an EDE Environment to Other Entities, for more information about the requirements related to upstream EDE Entities adding functionality or systems.

CMS considers Auditors to be downstream and delegated entities of the EDE Entity in accordance with 45 C.F.R. § 155.221(f). The EDE Entity is therefore responsible for its Auditor(s)'s performance and compliance with applicable EDE program requirements.

III. Information for Existing EDE Entities and Certain Prospective EDE Entities

A. EDE Entities That CMS Approved to Use the EDE Pathway

For existing EDE Entities that are not changing their EDE application phase for Year 7 of EDE or otherwise seeking to add new functionality or systems to their approved EDE environment, CMS aims to mitigate the burden of the EDE audit and agreement renewal process.

i. Business Requirements Audit

Prospective phase change EDE Entities should refer to Section XI.A.ii, EDE Entity-initiated Phase Change Requests, for the requirements and process to implement an EDE Entity-initiated

[15] Also see 45 C.F.R. § 155.220(k)(3).

[16] Generally, unless specifically indicated otherwise, references to the EDE Business Agreement or the ISA refer to the current, legally enforceable version of each agreement. As of the release of these Guidelines, CMS has released the PY 2024 versions of both Agreements, which will remain in effect until the day before the PY 2025 OEP. The EDE Business Agreement and ISA are available on CMS zONE at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment. These Agreements are typically updated on an annual basis, including to account for and align with updates to these Guidelines.

[17] QHP display changes are limited to issuer upstream EDE Entities. Please refer to Section IV.A, Providing an EDE Environment to Other Entities, for more information.

phase change request (CR). Phase CRs are governed by the audit requirements detailed in these Guidelines and the associated baseline business requirements audit toolkits.[18] A primary EDE Entity that wants to make significant changes to their approved EDE environment, such as by adding functionality or systems,[19] should refer to Section XI.A, EDE Entity-initiated Change Requests, for applicable requirements and processes. Existing EDE Entities that are not pursuing a different EDE phase or otherwise seeking to make significant changes to their approved EDE environment do not need to contract with an Auditor to conduct and submit a new business requirements audit. Existing EDE Entities will need to continue to implement CMS-initiated CRs as described in Section XI.B, CMS-initiated Change Requests, of these Guidelines.

ii. Privacy and Security Audit

Existing EDE Entities that are required to submit a privacy and security audit (e.g., primary EDE Entities, hybrid issuer upstream EDE Entities with single sign-on, and hybrid non-issuer upstream EDE Entities) must adhere to the continuous monitoring reporting requirements in the *Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide* (ISCM Strategy Guide), which includes the completion of an annual assessment of security and privacy controls by an Auditor, as described in the ISCM Strategy Guide. A prospective phase change EDE Entity and existing primary EDE Entity that intends to make significant changes to an approved EDE environment (in addition to a phase change) should refer to Section XI.A, EDE Entity-initiated Change Requests, for applicable requirements and processes, which may include conducting a supplemental privacy and security audit.

Consistent with Section V of the guidance document *Updated Web-broker Direct Enrollment Program Participation Minimum Requirements* (published May 21, 2020), primary EDE Entities or hybrid non-issuer upstream EDE Entities that are web-brokers may submit one ISCM audit that covers the full scope of both the web-broker privacy and security continuous monitoring requirements and the EDE privacy and security continuous monitoring requirements.[20] Web-brokers exercising this option must submit an attestation to CMS consistent with Section V of that guidance document.

iii. Annual Agreement and Operational and Oversight Information Collection

Annually, prior to the OEP, CMS will contact prospective EDE Entities that have submitted audits and existing EDE Entities to submit the applicable components of the DE Entity Documentation Package, EDE Business Agreement, and the ISA (for primary EDE Entities

[18] As described in Section VI.B.ii, Business Requirements Audit Resources, CMS will identify baseline versions of each toolkit in early 2024; these baseline toolkits for each year comprise the earliest version of each toolkit that an EDE Entity could use in conducting a business requirements audit for the audit submission window for Year 7 of EDE.

[19] As we have previously explained, CMS generally considers the addition of functionality or systems to be significant changes to an approved EDE environment. However, changes that do not include the addition of functionality or systems may also constitute significant changes, such as modifications to the overall design of an audited and approved EDE Entity's eligibility application implementation or modifications to the IT infrastructure hosting an EDE environment. The *Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems* describes the EDE Entity-initiated change categories and is located on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

[20] The *Updated Web-broker Direct Enrollment Program Participation Minimum Requirements* guidance document is available at the following link: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/2020-WB-Program-Guidance-052120-Final.pdf.

only).[21] Exhibit 1 provides an overview of the minimum documentation and training requirements that are required for EDE Entities to receive countersigned Agreements from CMS during the annual EDE agreement process.[22]

Exhibit 1: Annual EDE Agreement Process Documentation Requirements

Document	Description	Submission Requirements	Entity Responsible
***DE Entity Documentation Package*—Privacy Questionnaire (or attestation, if applicable, see Submission Requirements column)**	▪ Primary EDE Entities must submit the privacy questionnaire. The privacy questionnaire collects information about what information is collected by the EDE Entities platforms, how that information is used, and which tracking technologies are utilized in order to assess any privacy impact to consumers. ▪ The privacy questionnaire form will be available on CMS zONE in the DE Entity Documentation Package ZIP file.	▪ Submit via the DE/EDE Entity Program Management Environment (PME) Site ▪ If an EDE Entity's responses to the privacy questionnaire are unchanged from the EDE Entity's last submission of a privacy questionnaire, the Entity may submit an attestation stating that the previously submitted questionnaire remains accurate. – The attestation must be on company letterhead with a signature from an officer with the authority to bind the EDE Entity to the contents.	Primary EDE Entity
***DE Entity Documentation Package*—Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements column)**	▪ The URL and text of each privacy policy statement displayed on the EDE Entity's website and the EDE Entity's website Terms of Service in a Microsoft Word document or a PDF. ▪ The privacy policy and Terms of Service must be submitted for any EDE Entity's website that collects consumer data as part of the EDE end-user experience.	▪ Submit via the DE/EDE Entity PME Site ▪ If an EDE Entity's privacy policy and Terms of Service remain unchanged from the EDE Entity's last submission of the privacy policy and Terms of Service, the Entity may submit an attestation stating that the previously submitted privacy policy and Terms of Service remain unchanged. – The attestation must be on company letterhead with a signature from an officer with the authority to bind the EDE Entity to the contents.	Primary and upstream EDE Entities

[21] Please refer to Section VI.B.i, Required Business Requirements Audit Documentation, for more information on the operational and oversight information that will be required by CMS as part of this annual process.

[22] EDE Entities must complete continuous monitoring requirements (e.g., ISCM) as described in Section III.A, EDE Entities That CMS Approved to Use the EDE Pathway, in order to receive countersigned Agreements from CMS.

Document	Description	Submission Requirements	Entity Responsible
***DE Entity Documentation Package*—Operational and Oversight Information Excel Form**	▪ EDE Entities must submit the operational and oversight information to CMS to use the EDE pathway. This form must be filled out completely. ▪ The form is a macro-enabled Excel file that the EDE Entity will complete and submit to CMS. Note: If the EDE Entity is unable to complete the macro-enabled form, follow the instructions in the Documentation Package to complete the form without enabling macros.	▪ Submit via the DE/EDE Entity PME Site. ▪ CMS will notify EDE Entities when the Operational and Oversight Information Excel Form is available during the EDE agreement renewal process, until that point, EDE Entities must use the current form in the DE Entity Documentation Package.	Primary and upstream EDE Entities
EDE Business Agreement	▪ EDE Entities must execute the EDE Business Agreement to use the EDE pathway. The agreement must identify the Entity's selected Auditor(s) (if applicable). ▪ For primary EDE Entities, CMS will countersign the EDE Business Agreement after CMS has reviewed and approved the EDE Entity's business requirements audit and the annual privacy and security audit. ▪ For upstream EDE Entities, CMS will countersign the EDE Business Agreement after the upstream EDE Entity's primary EDE Entity has received CMS approval, and CMS has reviewed the arrangement specific documentation, consistent with the Entity-initiated Change Request Process detailed in Section XI.A.i, EDE Entity-initiated Change Request Process.	▪ Submit via the DE/EDE Entity PME Site.	Primary and upstream EDE Entities

Document	Description	Submission Requirements	Entity Responsible
Interconnection Security Agreement (ISA)	▪ A primary EDE Entity must submit the ISA to use the EDE pathway. ▪ CMS will countersign the ISA after CMS has reviewed and approved the EDE Entity's business requirements audit and annual privacy and security audit.	▪ Submit the ISA via the DE/EDE Entity PME Site. ▪ The ISA contains Appendices that must be completed in full for an EDE Entity to be considered for approval. ▪ Appendix B of the ISA must detail: (1) all arrangements with upstream EDE Entities, relationship type, and any related data connections or exchanges, (2) any arrangements involving web-brokers, and (3) any arrangements with downstream agents and brokers that involve proposed additional functionality or systems including limited data collections with a secure redirect, as described in Section IV.B., Downstream Third-party Agent and Broker Arrangements. ▪ Appendix B of the ISA must be updated and resubmitted, with changes noted in the change log, when a primary EDE Entity adds or changes any of the arrangements noted above consistent with the requirements in the ISA.	Primary EDE Entities
Training	▪ EDE Entities must complete the trainings as outlined in Section VIII, Required Auditor and EDE Entity Training. ▪ The trainings are located on REGTAP (located at the following link: https://www.regtap.info/).	▪ The person taking the training must complete the course conclusion pages at the end of each module. ▪ The EDE Entity and Auditor are NOT required to submit anything additional to CMS but must retain a copy of the training confirmation webpage to provide to CMS, if requested.	Primary and upstream EDE Entities

B. EDE Entities That Have Completed Their Audits, but That CMS Has Not Approved

i. Business Requirements Audit

For a prospective EDE Entity that has not been approved for PY 2024 but has submitted a complete business requirements audit prior to the release of these Guidelines and entered the audit queue, CMS will allow such a prospective EDE Entity to use its previously submitted and complete business requirements audit assuming it continues to seek approval for the phase indicated in its initial audit submission, and it does not otherwise seek to make significant changes[23] to its EDE environment prior to approval. A prospective primary EDE Entity that intends to add functionality or systems or otherwise make changes to an audited EDE

[23] The *Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems* describes the EDE Entity-initiated change categories and is located on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

environment should refer to Section XI.A, EDE Entity-initiated Change Requests, for applicable requirements and processes, which may include conducting a supplemental audit. The prospective EDE Entity must implement any changes to the business requirements as detailed in Section XI.B, CMS-initiated Change Requests. CMS will only allow this approach to the extent that the previous audit accurately represents review of a prospective EDE Entity's currently configured EDE environment.

ii. Privacy and Security Audit

For a prospective EDE Entity that is not approved for PY 2024 but has submitted a complete privacy and security audit prior to the release of these Guidelines and entered the audit queue, CMS will allow such a prospective EDE Entity to use its previously submitted privacy and security audit. The audit must have been submitted no more than one year prior to the date of the prospective EDE Entity's approval by CMS for it to serve as the basis of approval; otherwise, CMS will require additional privacy and security documentation to provide an accurate and timely evaluation of the EDE environment prior to approval (e.g., an audit submission consistent with the ISCM Strategy Guide). In addition, no significant changes may have been made to the EDE Entity's environment since the submission of the audit pursuant to the processes defined below in Section XI, Processes for Changes to an Audited or Approved EDE Environment. CMS will only allow this approach to the extent that the previous privacy and security audit accurately represents review of a prospective EDE Entity's currently configured EDE environment. Consistent with the ISCM Strategy Guide, prospective EDE Entities may need to provide updated privacy and security documentation to CMS to demonstrate the continued compliance of their EDE environments.

C. EDE Entities That Have Submitted an Incomplete Audit During the Prior Audit Submission Window

i. Business Requirements Audit

Prospective EDE Entities that submitted incomplete audit documentation during the Year 6 audit submission window and wish to pursue EDE approval in Year 7 of EDE must undergo a new business requirements audit consistent with the requirements in these Guidelines. Prospective EDE Entities in this situation must have an Auditor complete a business requirements audit using the updated business requirements audit baseline toolkits referenced in these Guidelines and submit the associated documentation during the Year 7 audit submission window.

ii. Privacy and Security Audit

Prospective EDE Entities that submitted incomplete audit documentation during the Year 6 audit submission window and wish to pursue EDE approval in Year 7 of EDE must undergo a new privacy and security audit consistent with the requirements in these Guidelines. Prospective EDE Entities in this situation must have an Auditor complete a privacy and security audit consistent with the updated requirements documented in these Guidelines and submit the associated documentation during the Year 7 audit submission window.

D. Primary EDE Entities That CMS Has Approved to Use the EDE Pathway, but That Have Not Utilized the EDE Pathway in Production

Primary EDE Entities that CMS has approved to use the EDE pathway, but that have not utilized the EDE pathway in production (e.g., a primary EDE Entity that built an EDE platform only to

facilitate use of the EDE pathway by upstream EDE Entities and that has not finalized arrangements with any such entities) within one year of the initial execution of their EDE Business Agreements and ISAs must demonstrate operational readiness and compliance with applicable requirements prior to the EDE Entity's EDE environment being used to complete an Exchange eligibility application or a QHP selection. This includes complying with any additional steps and processes necessary to confirm compliance with current requirements. If an EDE Entity is in this situation, CMS may withhold execution of subsequent EDE agreements during agreement renewal or delay the approval of an upstream EDE Entity until these additional program integrity and risk mitigation steps and processes have been met to CMS's satisfaction.

At a minimum, a primary EDE Entity that has not utilized the EDE pathway in production within one year of the initial execution of its EDE Business Agreement and ISA must meet the following criteria:

1) Complete CMS-designated API Functional Integration Toolkit test cases and submit related documentation as required by the Toolkit,[24] and resolve any risks identified by CMS during its review of the submitted documentation;
2) Remain current on CMS-initiated Change Requests;[25] and
3) Complete an eligibility application mini audit[26] and resolve any risks identified by CMS.

CMS will communicate to a primary EDE Entity the additional criteria, if any, that must be met to receive approval to utilize the EDE pathway in production. This information will be communicated in writing to the EDE Entity at the time that CMS notifies the EDE Entity that it must demonstrate operational readiness and compliance with applicable requirements prior to using the EDE pathway in production.

Upon successful completion of the steps described above and other applicable criteria CMS identifies, CMS may approve the primary EDE Entity to utilize the EDE pathway in production and/or execute the EDE Business Agreement and ISA, if necessary. If, after being re-approved under the processes described in this subsection, a primary EDE Entity has not utilized the EDE pathway in production within one year of their re-approval to use the EDE pathway in production, the EDE Entity must again demonstrate operational readiness and compliance with applicable requirements, consistent with this subsection, prior to using the EDE pathway to complete an Exchange eligibility application or a QHP selection.

IV. Enhanced Direct Enrollment Arrangements

EDE Entities have several options to consider in determining how and to what extent to participate in EDE. An Entity may seek to participate as a primary EDE Entity that has developed its own EDE environment, as an upstream EDE Entity leveraging an approved

[24] The relevant Toolkit for meeting this requirement will be the baseline Toolkit released for the most recent or current audit submission window.
[25] CMS-initiated Change Requests are detailed and tracked on CMS zONE at the following link: https://zone.cms.gov/document/business-audit.
[26] Mini audits are described in more detail in Sections X.E, Final Approval Process, and X.F, Post-EDE-Approval Oversight Processes.

primary EDE Entity's EDE environment, or as a downstream agent/broker using a primary EDE Entity's or upstream EDE Entity's EDE environment.

A. Providing an EDE Environment to Other Entities[27]

A primary EDE Entity is an entity that develops, designs, and hosts its own EDE environment for its own use or for use by others. A primary EDE Entity must have a third-party Auditor complete the business requirements and privacy and security audits, sign the ISA and EDE Business Agreement, have its own Partner ID, and comply with all applicable requirements, including conducting oversight of upstream EDE Entity and downstream agent and broker users of its approved EDE environment. An upstream EDE Entity is an entity that uses an EDE environment provided by a primary EDE Entity.[28] All upstream EDE Entities must have a legal relationship with a primary EDE Entity reflected in a signed written agreement between the upstream EDE Entity and the primary EDE Entity. There are three categories of upstream EDE Entities: white-label issuers; hybrid issuers; and hybrid, non-issuers. For all upstream arrangements, the "EDE end-user experience" consists of all aspects of the pre-application, application, plan shopping, plan selection, enrollment, and post-enrollment experience and any data[29] collected necessary for those steps or for the purposes of any Authorized Functions.[30, 31] CMS allows for unique white-label branding and logos within the primary EDE Entity's environment for all upstream arrangements.[32] Only a primary EDE Entity can provide an EDE environment to an upstream Entity ; that is, upstream EDE Entities cannot provide an EDE environment to other upstream EDE Entities.

The primary EDE Entity must detail all arrangements with upstream EDE Entities by submitting an Entity-initiated Change Request, consistent with Section XI.A, EDE Entity-initiated Change Requests, and a completed ISA Appendix B that details the arrangements and any data connections or exchanges. If a primary EDE Entity is unclear on whether an arrangement needs to be included, the primary EDE Entity should submit an Appendix B detailing the arrangement to CMS or contact CMS to discuss the arrangement to confirm if it needs to be reported.

---

[27] This section does not address requirements related to non-issuer white-label users (also referred to as downstream agents and brokers) of a primary EDE Entity's EDE environment. Please refer to Section IV.B, Downstream Third-party Agent and Broker Arrangements, for more information on these types of arrangements.

[28] The list of EDE Entities (both primary and upstream) that are approved to use EDE is available at the following link: https://www.cms.gov/programs-and-initiatives/health-insurance-marketplaces/direct-enrollment-and-enhanced-direct-enrollment (see "Approved EDE Entities List").

[29] All subsequent references to "data" collected in this document are inclusive of the data elements delineated in Section III.a, "Authorized Functions," of the EDE Business Agreement, which is available on CMS zONE at the following link: https://zone.cms.gov/document/business-audit.

[30] Collectively, CMS considers these elements to constitute the EDE end-user experience whether the end-users are consumers or agents or brokers.

[31] For a list of Authorized Functions for which an EDE Entity may create, collect, disclose, access, maintain, store, and use a consumer's personally identifiable information, please refer to Section III.a, "Authorized Functions", of the EDE Business Agreement, which is available on CMS zONE at the following link: https://zone.cms.gov/document/business-audit.

[32] See Section IV.B, Downstream Third-party Agent and Broker Arrangements, for information on what types of branding is permitted in these downstream arrangements.

Furthermore, any arrangements involving web-brokers must be detailed in an Appendix B submission.[33]

As noted in Section VII of the EDE Business Agreement, an issuer EDE Entity's signatory on the EDE Business Agreement must have sufficient authority to execute an agreement with CMS on behalf of the issuer EDE Entity and all affiliated issuer organizations that use the issuer EDE Entity's EDE environments or EDE end-user experiences. Issuer EDE Entities must identify all applicable affiliated issuer organizations in the "Operational and Oversight Information" form provided by CMS in the DE Entity Documentation Packages.[34]

Please review Section XI.A, EDE Entity-initiated Change Requests, for the necessary steps to submit an EDE Entity-initiated Change Request to initiate onboarding an upstream EDE Entity. A primary EDE Entity may submit an EDE Entity-initiated Change Request for a proposed upstream EDE Entity arrangement at any time after the primary and upstream EDE Entities have established a legal relationship and agreed on the technical implementation and End-user Experience for the EDE Environment, including any proposed additional functionality or systems.

i. White-label Issuer Upstream EDE Entities

White-label issuers are upstream EDE Entities that use a primary EDE Entity's approved EDE environment, but make minor branding and QHP display changes to facilitate their use of the other Entity's approved EDE environment. White-label issuers may add their logos and otherwise re-brand the EDE environment to present it as their own, and may limit their plan displays to their own QHP offerings consistent with 45 C.F.R. § 156.1230(a)(1)(ii).[35] White-label issuer upstream EDE Entities must otherwise use the primary EDE Entity's environment without modification and cannot add any functionality or systems to the primary EDE Entity's approved EDE environment. If a white-label issuer upstream EDE Entity intends to add additional functionality or systems, the white-label issuer upstream EDE Entity must follow the process in Section XI.A, EDE Entity-initiated Change Requests. Upon approval to add additional functionality or systems, the white-label issuer upstream EDE Entity would become a hybrid issuer upstream EDE Entity. White-label issuer upstream EDE Entities are not required to conduct and submit a business requirements audit or a privacy and security audit, but they must submit the applicable components of the DE Entity Documentation Package (as described in VI.B, Audit Documentation), as well as the EDE Business Agreement, and they must also maintain a unique Partner ID.

ii. Hybrid Issuer Upstream EDE Entities

A hybrid issuer upstream EDE Entity is an issuer that implements—or has a primary EDE Entity implement on its behalf—additional functionality or systems to the primary EDE Entity's EDE environment beyond minor branding changes or QHP display changes. CMS considers any

[33] As noted in Section IV.B, Downstream Third-party Agent and Broker Arrangements, any arrangements involving web-brokers must be detailed in an ISA Appendix B submission for review by CMS even if they are believed to be pure white-label arrangements.

[34] Please refer to Section VII of the EDE Business Agreement, which is available at CMS zONE at the following link: https://zone.cms.gov/document/business-audit.

[35] Please refer to Section IV.D, QHP Shopping Experience in an EDE Environment, for more information.

changes to a primary EDE Entity's approved EDE environment or the overall EDE end-user experience beyond minor branding changes or QHP display changes to be the addition of functionality or systems to an approved EDE environment. For example, additional functionalities or systems may include any redirect or connection to another entity's system or website (e.g., the hybrid, issuer upstream EDE Entity's system or website) as part of the EDE pre-application, application, plan shopping, plan selection, enrollment, or post-enrollment experience, including any data collection prior to initiating or after completing the Exchange application and/or submitting the QHP enrollment to the applicable Exchange.

If the primary EDE Entity intends to share data with a hybrid issuer upstream EDE Entity, this must be documented in the primary EDE Entity's ISA Appendix B. This includes, for example, if the hybrid issuer upstream EDE Entity is hosting its own QHP shopping experience and collects and sends consumer data to, or receives consumer data from, the primary EDE Entity outside the boundaries of the primary EDE Entity's approved EDE environment.

Hybrid issuer upstream EDE Entities that utilize Single Sign-On (SSO) are required to retain an Auditor to conduct a supplemental privacy and security audit consistent with the requirements described in Section IV.A.v, Privacy and Security Audit Requirements for Hybrid Issuer Upstream EDE Entities Implementing Single Sign-On.

Hybrid issuer upstream EDE Entities must sign an EDE Business Agreement and maintain a unique Partner ID. Entities that have questions regarding hybrid issuer upstream EDE arrangements should contact DE Support at directenrollment@cms.hhs.gov.

iii. Hybrid Non-Issuer Upstream EDE Entities

Hybrid non-issuer upstream EDE Entities are agents, brokers, or web-brokers that use a primary EDE Entity's EDE environment consistent with the standards of this section. A hybrid non-issuer upstream EDE Entity arrangement may be primarily characterized by the presence of additional functionality or systems that modify or represent additions to the primary EDE Entity's EDE environment beyond minor branding changes or otherwise change the EDE end-user experience. The hybrid non-issuer upstream EDE Entity arrangement may have split control or authority for creating and/or maintaining the systems and functionality that comprise the totality of the EDE environment or end-user experience. For example, additional functionalities or systems may include any redirect or connection to another entity's system or website (e.g., the hybrid non-issuer upstream EDE Entity's system or website) as part of the EDE pre-application, application, plan shopping, plan selection, enrollment, or post-enrollment experience, including any data collection prior to initiating or after completing the Exchange application and/or submitting the QHP enrollment to the applicable Exchange. In addition, the use of single sign-on to facilitate seamless access to different systems as end users are redirected between systems may also be characteristic of a hybrid non-issuer upstream EDE Entity arrangement.

One key criterion that CMS will consider in evaluating relationships between primary EDE Entities and potential hybrid non-issuer upstream EDE Entities is the transference of a consumer's experience or a consumer's data outside of the boundaries of a primary EDE Entity's approved environment. For example, CMS would consider any arrangement that transmits a consumer's data—either collected from the consumer for Exchange application and QHP enrollment purposes or provided by the Exchange pursuant to such activities—outside the system

boundaries of a primary EDE Entity's approved EDE environment to constitute a hybrid non-issuer upstream EDE Entity arrangement. The following examples illustrate situations that CMS would consider constituting a hybrid non-issuer upstream EDE Entity relationship with a primary EDE Entity:

- Example Scenario 1: A hybrid non-issuer upstream EDE Entity displays QHPs to the consumer separate from the primary EDE Entity's EDE environment and then redirects the consumer and/or their data to the primary EDE Entity for completing the eligibility application or submitting the enrollment transaction to the applicable Exchange.
- Example Scenario 2: A hybrid non-issuer upstream EDE Entity provides a plan selection and enrollment process separate from the primary EDE Entity's EDE environment. This may involve any exchange of applicable consumer data (pre-application or post-application) between the hybrid non-issuer upstream EDE Entity's system(s) and the primary EDE Entity's EDE environment to complete plan selection and enrollment. The consumer or the consumer's data may then be relayed back to the primary EDE Entity's EDE environment for further action, including enrollment, post-enrollment communications, and post-enrollment management action items.
- Example Scenario 3: A hybrid non-issuer upstream EDE Entity retrieves, stores, transfers, or manages consumer data obtained or collected through the primary EDE Entity's EDE environment outside of that environment (e.g., data stored by customer relationship management software hosted or maintained outside of the primary EDE Entity's EDE environment for the hybrid non-issuer upstream EDE Entity's use).

These Guidelines do not provide examples of the full universe of possible hybrid non-issuer upstream EDE Entity relationships or arrangements.[36] For example, any arrangement where a non-issuer upstream entity implements an EDE program requirement instead of the primary EDE Entity (e.g., privacy and security controls, business requirements, Agent and Broker identity proofing, etc.) would likely be a hybrid non-issuer upstream EDE Entity arrangement.

For purposes of analyzing whether there is a hybrid non-issuer upstream EDE Entity arrangement, the scope of the evaluation covers the full EDE end-user experience. This includes any data collected or received from the Exchange or Exchange consumers (directly or indirectly via an agent or broker), any implementation of the EDE requirements, any preliminary QHP shopping or eligibility information or estimates, and the QHP selection and enrollment experience. Depending on the additional functionality and systems added to the EDE end-user experience, the hybrid non-issuer upstream EDE Entity may also need to onboard and register with CMS as a web-broker. For example, a hybrid non-issuer upstream EDE Entity that hosts its own QHP display or plan shopping experience as part of the EDE end-user experience must be registered with CMS as a web-broker.

If a non-issuer entity only redirects a consumer from its website to a primary EDE Entity's EDE environment to complete the EDE end-user experience, and the entity does not exchange any

[36] Primary EDE Entities or hybrid non-issuer upstream EDE Entities that have questions regarding permissible arrangements and the hybrid non-issuer upstream EDE Entity model should contact DE Support at directenrollment@cms.hhs.gov.

data or provide any Exchange-related information relevant to the EDE end-user experience, then it would not be considered a hybrid non-issuer upstream EDE Entity relationship.[37]

As detailed further below, hybrid non-issuer upstream EDE Entities are required to retain an Auditor to conduct a privacy and security audit relevant to the additional functionalities or systems it seeks to add to the primary EDE Entity's approved EDE environment. Hybrid non-issuer upstream EDE Entities must also sign an EDE Business Agreement and maintain a unique Partner ID.

iv. Privacy and Security Audit Requirements for Hybrid Non-issuer Upstream EDE Entities

A prospective hybrid non-issuer upstream EDE Entity must complete an ORR[38] that includes a privacy and security audit conducted by an Auditor.[39] This audit must be conducted in compliance with the requirements for a primary EDE Entity conducting a privacy and security audit outlined in Sections V, Selection of an Auditor; VII, Privacy and Security Audit Requirements and Scope; VIII, Required Auditor and EDE Entity Training; and X, Approval Process and Audit Submission Window.[40] The Auditor must evaluate the prospective hybrid non-issuer upstream EDE Entity's compliance with all applicable EDE privacy and security controls and requirements;[41] however, the Auditor does not need to independently evaluate the implementation of any inherited common controls implemented by the primary EDE Entity.[42] Instead, the Auditor only needs to validate that the controls labeled as "inherited common controls" are applicable to the hybrid non-issuer upstream EDE Entity's EDE environment. The Auditor, however, must verify that all non-inherited and hybrid controls[43] are fully implemented and document any controls that have not been implemented. The Auditor must document any related mitigation steps the prospective hybrid non-issuer upstream EDE Entity has taken. These requirements are consistent with the instructions in the Non-Exchange Entity (NEE) System Security and Privacy Plan (SSP) Template.[44] For a list of all of the privacy and security controls applicable to hybrid non-issuer upstream EDE Entities (including the ones that may be inherited from the primary EDE Entity), please refer to Exhibit 12 and Exhibit 13 in Appendix A of these Guidelines. Prospective hybrid non-issuer upstream EDE Entities must submit their Auditor

[37] Such an arrangement would be considered to be a downstream agent or broker arrangement. See Section IV.B, Downstream Third-party Agent and Broker Arrangements for additional examples of the types of arrangements that would be considered downstream agent or broker arrangements, rather than hybrid non-issuer upstream EDE Entity arrangements.

[38] See 45 C.F.R. § 155.221(b)(4) and (f).

[39] A hybrid non-issuer upstream EDE Entity may leverage prior audit results that assessed some or all control requirements listed in Exhibit 12 and Exhibit 13 of Appendix A if the prior audit was conducted within one year of the date the hybrid non-issuer upstream EDE Entity submits its audit documentation to CMS.

[40] Hybrid non-issuer upstream EDE Entity privacy and security audits and business requirements audits (if applicable) may be submitted on a rolling basis. The audit(s) must be complete for the Entity to enter the CMS audit review queue. Resubmissions of audit documentation to provide missing elements not included in a previous submission may similarly be submitted on a rolling basis.

[41] For a list of privacy and security controls that the Auditor must evaluate to ensure compliance by the hybrid non-issuer upstream EDE Entity, please refer to Exhibit 12 in Appendix A of these Guidelines.

[42] For a list of inheritable common controls, please refer to Exhibit 13 in Appendix A of these Guidelines.

[43] Non-inherited controls include any inheritable common controls that have not been inherited from the primary EDE Entity's EDE environment.

[44] See page iv of the NEE SSP available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

contracts, SAPs, and NEE SSPs, as well as participate in audit kick-off calls with CMS prior to initiating their audits. CMS may schedule status calls with prospective hybrid non-issuer upstream EDE Entities that have submitted complete privacy and security audits until they are approved. Please refer to Section X.G, Approval Process for Upstream EDE Entities with Audit Requirements, for more information on the audit review process for upstream EDE Entities.

After CMS approves a hybrid non-issuer upstream EDE Entity, the EDE Entity must implement and maintain an ISCM program for its systems to maintain CMS approval. The ISCM requirements are detailed in the EDE Guidelines and the ISCM Strategy Guide (available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit).

Hybrid non-issuer upstream EDE Entities must also comply with the business audit post-approval activities described in Section XI, Processes for Changes to an Audited or Approved EDE Environment, as applicable (e.g., if the hybrid non-issuer upstream EDE Entity has implemented some portion of the EDE Business Requirements outside of the primary EDE Entity's EDE environment, such as the Agent and Broker identity proofing or post-eligibility application communications, it must adhere to the applicable CR requirements).

A primary EDE Entity that wants to enter into an arrangement with a hybrid non-issuer upstream EDE Entity must initiate the process for a category 3 EDE Entity-initiated Change Request as described in Section XI, Processes for Changes to an Audited or Approved EDE Environment. CMS recommends that a primary EDE Entity submit documentation for the category 3 EDE Entity-initiated Change Request before the hybrid non-issuer upstream EDE Entity initiates its audit. CMS will accept privacy and security audit submissions for hybrid non-issuer upstream EDE Entities on a rolling basis.

v. Privacy and Security Audit Requirements for Hybrid Issuer Upstream EDE Entities Implementing Single Sign-On

A hybrid issuer upstream EDE Entity must complete a supplemental privacy and security audit conducted by an Auditor if implementing a single sign-on solution, prior to their approval. A hybrid issuer upstream EDE Entity implementing a single sign-on solution must have their primary EDE Entity submit to CMS an updated ISA Appendix B and EDE Entity-initiated Change Request, see Section XI.A, EDE Entity-initiated Change Requests, that details the EDE Entity's proposed upstream EDE Entity arrangement. CMS will accept privacy and security audit submissions for hybrid issuer upstream EDE Entities implementing single sign-on on a rolling basis. This audit must be conducted in compliance with the requirements for a primary EDE Entity conducting a privacy and security audit outlined in Sections V, Selection of an Auditor; VII, Privacy and Security Audit Requirements and Scope; VIII, Required Auditor and EDE Entity Training; and X, Approval Process and Audit Submission Window.[45] The Auditor must evaluate the hybrid issuer upstream EDE Entity's compliance with all applicable EDE privacy and security controls documented in Appendix A, Exhibit 14. The Auditor does not need to independently evaluate the implementation of any inherited common controls implemented by

[45] Hybrid issuer upstream EDE Entity privacy and security audits and business requirements audits (if applicable) may be submitted on a rolling basis. The audit(s) must be complete for the Entity to enter the CMS audit review queue. Resubmissions of audit documentation to provide missing elements not included in a previous submission may similarly be submitted on a rolling basis.

the primary EDE Entity.[46] Instead, the Auditor only needs to validate that the controls labeled as "inherited common controls" are applicable to the hybrid issuer upstream EDE Entity's EDE environment. The Auditor must, however, verify that all non-inherited and hybrid controls in Exhibit 14 are fully implemented and document any controls that have not been implemented.[47] A hybrid issuer upstream EDE Entity implementing single sign-on may leverage prior audit results that assessed some or all control requirements listed in Exhibit 14 if the prior audit was conducted within one year of the date the hybrid issuer upstream EDE Entity is submitting its audit documentation to CMS. The Auditor must document any related mitigation steps the hybrid issuer upstream EDE Entity has taken. These requirements are consistent with the instructions in the NEE SSP Template.[48] Hybrid issuer upstream EDE Entities implementing single sign-on must submit their Auditor contract and SAP, as well as participate in an audit kick-off call with CMS prior to initiating their audits. Please refer to Section X.G, Approval Process for Upstream EDE Entities with Audit Requirements, for more information on the audit review process for upstream EDE Entities.

After CMS approves a hybrid issuer upstream EDE Entity implementing single sign-on, the EDE Entity must implement and maintain an ISCM program for its systems to maintain CMS approval. The ISCM requirements are detailed in these Guidelines and the ISCM Strategy Guide.[49]

Additionally, if the hybrid issuer upstream EDE Entity implementing single sign-on will be implementing Agent/Broker or Consumer Identity Proofing—or any other business requirements functionality—the hybrid issuer upstream EDE Entity will need to submit a business audit report detailing the Auditor's assessment of the issuer's compliance with those requirements, consistent with Exhibit 2 and Section VI.B, Audit Documentation.

vi. Additional Standards Regarding Primary EDE Entities and Upstream EDE Entities

CMS requires written confirmation from both primary EDE Entities and their upstream Entities about any such relationships, as well as requires information and documentation from the upstream EDE Entities as requested, before allowing a connection to the EDE APIs on behalf of an upstream EDE Entity. Additionally, primary EDE Entities must identify inheritable common and hybrid security and privacy controls that their upstream EDE Entities should leverage. The common and hybrid security and privacy controls must be documented in the NEE SSP Template, and must also be documented as part of the written contract between primary EDE Entities and their upstream EDE Entities.[50]

[46] For a list of inheritable common controls, please refer to Exhibit 13 in Appendix A of these Guidelines.
[47] Non-inherited controls include any inheritable common controls that have not been inherited from the primary EDE Entity's EDE environment.
[48] See page iv of the NEE SSP Template available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.
[49] The ISCM Strategy Guide is available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.
[50] As white-label issuer upstream EDE Entities have not implemented any additional functionality or systems, primary EDE Entities do not need to document common and hybrid security and privacy controls in the written contract with a white-label upstream EDE Entity.

vii. Unique Partner ID Requirements for Primary EDE Entities and Upstream Entities

CMS requires primary EDE Entities with upstream EDE Entities to submit EDE API transactions using Partner IDs associated with the upstream EDE Entities when EDE applications/enrollments originate from an upstream EDE Entity.[51] This requirement applies to all types of upstream EDE Entities (including white-label and hybrid arrangements).

CMS requires this for the following reasons:

- For reporting and tracking purposes, the application/enrollment must reflect the EDE Entity that the transaction originated from.
- For purposes of suspension, if applicable, CMS can suspend specific Partner IDs. If only one Partner ID is used by the primary EDE Entity, a suspension of either the primary EDE Entity or any single upstream EDE Entity would result in the suspension of all activity from any EDE Entity using that Partner ID.

A primary EDE Entity that has upstream EDE Entities must update its Hub[52] Onboarding Form to include additional information for each of its upstream EDE Entities. The Hub Onboarding Form can be found on CMS zONE,[53] and when completed, must be emailed to the email address included on CMS zONE and in the Hub Onboarding Form (Hubsupport@sparksoftcorp.com). Each upstream EDE Entity must have a unique Partner ID and will receive its Partner ID when it (or its primary EDE Entity) submits or updates its Hub Onboarding Form.

B. Downstream Third-party Agent and Broker Arrangements

i. General Downstream Agent and Broker Requirements

An EDE Entity may allow third-party agents and brokers who are validly registered with the FFE to use its approved EDE environment, either directly through the primary EDE Entity or by way of an arrangement with an upstream EDE Entity, to assist consumers in supported states (i.e., states in which the EDE Entity operates) with applying for coverage offered through an Exchange, as well as applying for Advanced Payments of the Premium Tax Credit (APTC) and Cost-Sharing reductions (CSRs), and with selecting QHPs. This includes agents and brokers that are also web-brokers in the context of classic DE but that are operating solely as agents and brokers in the context of using the EDE pathway.[54]

[51] CMS does not require a unique Partner ID for any downstream agent or broker arrangements. Please refer to Section IV.B, Downstream Third-party Agent and Broker Arrangements for more information on these types of arrangements.

[52] EDE Entities must connect to the Data Services Hub ("Hub") in order to access and use the Exchange APIs.

[53] The Hub Onboarding Form is available at the following CMS zONE webpage: https://zone.cms.gov/document/hub-onboarding-form.

[54] In other words, web-brokers that currently participate in classic DE can enter into an arrangement to use a primary EDE Entity's EDE environment. Depending on if there is additional functionality or systems provided by the primary EDE Entity to the web-broker, the arrangement may be a considered a downstream third-party agent and broker arrangement (see Section IV.B, Downstream Third-party Agent and Broker Arrangements) or a hybrid non-issuer upstream EDE Entity arrangement (see Section IV.A.iii, Hybrid Non-Issuer Upstream EDE Entities).

ii. Downstream Agent and Broker White-label User Arrangement Requirements

Downstream third-party agent and broker arrangements may be white-label arrangements for which a primary EDE Entity enables the downstream agent or broker to only make minor branding changes to the primary EDE Entity's EDE environment (i.e., adding an agent's or broker's logo or name to an EDE environment). Downstream third-party agent and broker arrangements that involve additional functionality or systems, except as detailed in this Section, would constitute hybrid non-issuer upstream EDE Entity arrangements requiring a privacy and security audit, at a minimum, consistent with Section IV.A.iii, Hybrid Non-Issuer Upstream EDE Entities. All agent and broker arrangements involving additional functionality or systems must be documented in the primary EDE Entity's ISA Appendix B.

If a downstream agent or broker only redirects a consumer from its website to a primary EDE Entity's EDE environment to complete the EDE end-user experience, and the primary EDE Entity does not exchange any data or provide any Exchange-related information relevant to the EDE end-user experience to the downstream agent or broker, then it would not be considered a hybrid non-issuer upstream EDE Entity relationship. However, a downstream agent or broker may collect limited data from a consumer on its own website and securely transmit it to an EDE Entity without necessarily making the arrangement a hybrid non-issuer upstream EDE Entity relationship. The following are examples of the types of data that may be collected and transmitted by the downstream agent or broker consistent with this approach. Information may be collected:

- To determine if a consumer is (or should be) shopping for QHPs, such as basic information to assess eligibility for financial assistance, as well as to estimate premiums (e.g., household income, ages of household members, number of household members, and tobacco use status).[55]
- Related to the consumer's service area (e.g., zip code, county, and state).

The data noted above may be securely transmitted by the downstream agent or broker and used in the EDE end-user experience without making the arrangement a hybrid non-issuer upstream EDE Entity relationship only if the data is transmitted in conjunction with the initial redirect of the consumer to the EDE end-user experience provided by the primary EDE Entity and the arrangement does not otherwise constitute a hybrid non-issuer upstream EDE Entity relationship as described above in Section IV.A.iii, Hybrid Non-Issuer Upstream EDE Entities. In any such arrangement, the data must be transmitted securely and in one direction only (i.e., from the downstream agent or broker to the primary EDE Entity's environment). This flexibility does not allow for a primary EDE Entity to send consumer data to the downstream agent or broker outside of the EDE end-user experience and does not allow for additional data exchanges beyond what is outlined above which takes place in conjunction with the initial redirect prior to the beginning of the EDE end-user experience on the primary EDE Entity's platform.

Any implementation consistent with what is described in this subsection (i.e., Section IV.B.ii, Downstream Agent and Broker White-label User Arrangement Requirements) must be

[55] As discussed in Section IV.A.iii, Hybrid Non-Issuer Upstream EDE Entities, providing a QHP shopping experience followed by a redirect would constitute a hybrid non-issuer upstream EDE Entity relationship. See Example Scenario 1.

documented within the primary EDE Entity's ISA Appendix B, including an identification of the data transferred with the redirect from the non-issuer entity's website, and submitted as an EDE Entity-initiated Change Request (see Section XI, Processes for Changes to an Audited or Approved EDE Environment), if CMS has already approved the primary EDE Entity's EDE environment.

Downstream third-party agents and brokers will not sign an EDE Business Agreement or the ISA and will not be provided or allowed to use a unique Partner ID for EDE API transactions.

Finally, for details regarding any additional user interface customization beyond the white-label branding described above, please refer to the EDE Entity-initiated Change Request process in Section XI, Processes for Changes to an Audited or Approved EDE Environment.

iii. Oversight of Downstream Agents and Brokers

An EDE Entity is responsible for ensuring compliance with applicable requirements, including the applicable terms and conditions of the EDE Business Agreement, by all downstream agents and brokers who access and use its approved EDE environment. An EDE Entity's environment must contain sufficient privacy and security safeguards and must be accessed consistent with its documented policies and procedures, to protect against noncompliance by any authorized downstream agents and brokers who are using its EDE environment or interacting with or managing any consumer applications associated with its EDE environment. For example, while CMS does not require downstream agents or brokers who use an EDE Entity's EDE environment to sign the ISA independently, CMS does require that the written agreement between the EDE Entity and its downstream agents or brokers require the agent or broker to comply with the relevant and applicable privacy and security requirements contained within Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities to the Agreement between Agent or Broker and the Centers for Medicare & Medicaid Services for Individual Market Federally-Facilitated Exchanges and the State-Based Exchanges on the Federal Platform. Furthermore, a compliant EDE environment that is appropriately managed by an EDE Entity must protect against noncompliant use of the environment by downstream agents or brokers with respect to EDE privacy and security standards. Finally, web-brokers that are approved primary EDE Entities, or approved hybrid non-issuer upstream EDE Entities, that allow the use of their EDE environments by downstream agents and brokers must comply with the requirements in 45 C.F.R. § 155.220(c)(4). Similarly, issuers that are approved primary or upstream EDE Entities and allow the use of their EDE environments by downstream agents and brokers must comply with the requirements in 45 C.F.R. § 156.340.[56]

C. Data Collections

An EDE Entity must perform data collections only within its approved EDE environment for purposes of the EDE pathway, except as approved by CMS through the EDE Entity-initiated Change Request process (see Section XI.A, EDE Entity-initiated Change Requests). Any and all websites that collectively make up an EDE Entity's EDE environment are subject to oversight by CMS. Any implementation or use of an EDE environment must be consistent with the audit(s) submitted to and approved by CMS.

[56] Downstream agents and brokers that use the EDE environment of an approved primary or upstream issuer EDE Entity are a type of delegated or downstream entity under 45 C.F.R. § 156.340.

D. QHP Shopping Experience in an EDE Environment

EDE Entities must comply with the applicable QHP display requirements for web-brokers and issuers as defined in 45 C.F.R. §§ 155.220, 155.221, and 156.1230. In the case of a primary EDE Entity allowing the use of its EDE environment by a white-label issuer upstream EDE Entity consistent with the provisions in Section IV.A, Providing an EDE Environment to Other Entities, the primary EDE Entity must provide an EDE environment that meets the QHP display requirements applicable to the white-label issuer upstream EDE Entity.[57] Similarly, if a primary EDE Entity provides the QHP display for a hybrid issuer upstream EDE Entity consistent with the provisions in Section IV.A, Providing an EDE Environment to Other Entities, the primary EDE Entity must provide an EDE environment that meets the QHP display requirements applicable to the hybrid issuer upstream EDE Entity.

If a primary EDE Entity allows the use of its EDE environment by downstream agents and brokers directly (i.e., not in the context of an upstream EDE Entity relationship) or by a hybrid non-issuer upstream EDE Entity that is not hosting its own plan shopping website (Section IV.A.iii, Hybrid Non-Issuer Upstream EDE Entities), the EDE environment must comply with the QHP display requirements applicable to the primary EDE Entity. In such situations—a downstream agent or broker or a hybrid non-issuer upstream EDE Entity that is not hosting its own plan shopping website—the primary EDE Entity may only make minor branding changes to the primary EDE Entity's EDE environment (i.e., adding an agent's or broker's logo or name to an EDE environment).[58]

In addition, CMS strongly recommends that EDE Entities offer the QHP selection experience after consumers have completed the eligibility application, as opposed to offering the QHP selection experience prior to a consumer completing the eligibility application. CMS recommends this to minimize the risk of a consumer's eligibility or plan availability changing after the consumer completes the eligibility application. For example, offering QHP selection prior to the eligibility application may motivate an EDE Entity to predict a consumer's eligibility for health insurance affordability programs (e.g., Medicaid, CHIP, APTC, and CSRs) based on very limited information, and ultimately the Exchange's eligibility determination may differ from the EDE Entity's prediction. As a result, consumers may be required to reassess their original QHP selections based on their official eligibility results from the Exchange. Additionally, if a consumer is completing a CiC, the consumer's plan availability may be restricted by Plan Category Limitations; however, the consumer and EDE Entity will not be aware of these potential limitations until the consumer has completed an eligibility application. As a result, consumers may not be eligible for the QHPs they initially selected.

---

[57] For example, a web-broker primary EDE Entity can provide a white-label issuer upstream EDE entity with an issuer-branded, white-label EDE environment that only displays the QHP issuer's plans consistent with 45 C.F.R. § 156.1230(a)(1)(ii). In such situations, the issuer branded white-label EDE environment would also display the disclaimer required under 45 C.F.R. § 156.1230(a)(1)(iv).

[58] For example, a web-broker primary EDE Entity would be required to display all QHPs offered through the applicable Exchange consistent with 45 C.F.R. § 155.220(c)(3)(i)(A), (B), and (D). This includes display of all QHP information provided by the Exchange or directly by the QHP issuer to the web-broker primary EDE Entity. The web-broker primary EDE Entity may only customize its website for a downstream agent or broker to include minor branding changes consistent with Section IV.B.ii, Downstream Agent and Broker White-label User Arrangement Requirements

V. Selection of an Auditor

A prospective EDE Entity that is subject to an audit requirement—including applicable hybrid issuer upstream EDE Entities (Section IV.A.v, Privacy and Security Audit Requirements for Hybrid Issuer Upstream EDE Entities Implementing Single Sign-On); hybrid non-issuer upstream EDE Entities (Section IV.A.iv, Privacy and Security Audit Requirements for Hybrid Non-issuer Upstream EDE Entities); prospective phase change EDE Entities (Section XI.A.ii, EDE Entity-initiated Phase Change Requests); and existing EDE Entities conducting an ISCM audit—must enter into a written agreement with each independent Auditor it selects. Pursuant to its oversight authority, CMS may request a copy of all documentation related to an EDE Entity's engagement of its Auditor(s) and the Auditor(s)' work in relation to the engagement. Each EDE Entity must identify its selected Auditor(s) in the EDE Business Agreement and the ISA between CMS and the EDE Entity. The EDE Entity must also submit a copy of the signed agreement or contract between the Auditor(s) and the EDE Entity to CMS. For more information, please review Section X.A, Pre-Audit Notification to CMS.

CMS will not provide EDE Entities with specific recommendations of Auditors to conduct an EDE audit. CMS encourages EDE Entities to work with their trade associations or other interested groups to share and disseminate information about possible Auditors that meet the criteria defined in this section of these Guidelines (Section V, Selection of an Auditor).

A. Allowance for Multiple Auditors

An EDE Entity is permitted to select either one Auditor to complete both the business requirements audit and the privacy and security audit or the EDE Entity may select two Auditors, one to complete the business requirements audit and the other to complete the privacy and security audit.

Consistent with Section X.A, Pre-Audit Notification to CMS, when an EDE Entity retains an Auditor(s), it must notify CMS as part of the pre-audit procedures and provide the contact information for the Auditor(s), including for the subcontractor(s) of an Auditor, if applicable. Additionally, the EDE Entity must provide CMS with the contract(s) between the EDE Entity and Auditor(s), as described in Section X.A, Pre-Audit Notification to CMS. Both the Auditor(s) and subcontractor(s) of the Auditor(s) will be considered downstream or delegated entities of the EDE Entity.[59] Auditors are permitted to subcontract these activities; however, an EDE Entity must disclose any subcontracting arrangements by its Auditor(s) in the EDE Business Agreement and/or ISA with CMS and disclose any potential conflicts of interest consistent with the EDE Business Agreement.

B. Business Requirements Auditor Experience

CMS requires that a prospective EDE Entity select an Auditor(s) with the experience outlined below and attest, within the EDE Business Agreement and the ISA, that the Auditor(s) have demonstrated or possess such experience.

[59] See 45 C.F.R. § 155.221(f).

i. Required Business Requirements Auditor Experience

CMS requires that the Auditor selected by a prospective EDE Entity to conduct the business requirements audit possess audit experience, which an Auditor may demonstrate through experience conducting operational audits or similar services for federal, state, or private programs. A prospective EDE Entity may consider an Auditor to be qualified to conduct the business requirements audit if key Auditor personnel possess one or more of the following relevant auditing certifications: Certified Internal Auditor (CIA), Certification in Risk Management Assurance (CRMA), Certified Information Systems Auditor (CISA), or Certified Government Auditing Professional (CGAP).

ii. Recommended Business Requirements Auditor Experience

CMS recommends that an Auditor conducting the business requirements audit has minimum technical experience with Extensible Markup Language (XML) and JavaScript Object Notation (JSON). Most of the new EDE APIs will be in JSON format; however, some will be in XML format. A general familiarity and understanding of XML and JSON request and response structure may be useful to an Auditor conducting the business requirements audit. The necessity of this experience may depend on the Auditor's approach to reviewing the prospective EDE Entity's environment and if the prospective EDE Entity provides information relevant to the audit in a user-friendly interface or in raw XML or JSON file format.

C. Privacy and Security Auditor Experience

i. Required Privacy and Security Auditor Experience

CMS requires that the key personnel of an Auditor selected by a prospective EDE Entity or an existing EDE Entity conducting an ISCM audit to conduct the privacy and security audit possess a combination of privacy and security experience and relevant auditing certifications. Examples of acceptable privacy and security experience include the following: 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) 18 System and Organization Controls (SOC) Report 2 experience; reviewing compliance with National Institute of Standards and Technology (NIST) SP 800-53 Revision 4 and 5, *Security and Privacy Controls for 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 Manager (CIPM), Certified Information Systems Security Professional (CISSP), Fellow of Information Privacy (FIP), HealthCare Information Security and Privacy Practitioner (HCISPP), CIA, Certified in Risk Management Professional (CRMP), CISA, or CGAP.

In determining whether an Auditor has an acceptable combination of privacy and security experience and relevant auditing certifications, an EDE Entity may substitute extensive FISMA experience for multiple privacy and security certifications.

The Auditor must be familiar with NIST standards, HIPAA, and other applicable federal privacy and cybersecurity regulations and guidance. In addition, the Auditor must be capable of performing penetration testing and vulnerability scans on all interfaces that collect personally identifiable information (PII) or connect to CMS.

ii. Recommended Privacy and Security Auditor Experience

CMS strongly recommends that an Auditor selected to conduct the privacy and security audit have prior FISMA experience and/or is listed on the FedRAMP-certified third-party assessment organization website.[60] Prior FISMA experience is recommended in order for an Auditor to appropriately assess an EDE Entity's compliance with the required privacy and security controls and produce a high-quality comprehensive Security and Privacy Controls Assessment Test Plan (SAP) and Security and Privacy Assessment Report (SAR).

D. Conflict of Interest and Auditor Independence and Objectivity

i. Conflict of Interest

An EDE Entity that is contracting with an Auditor to submit an audit to CMS must select an Auditor who is free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. An EDE Entity and its Auditor must disclose to HHS any financial relationship between the Auditor and individuals who own or are employed by the EDE Entity or who own or are employed by the EDE Entity for which the Auditor is conducting an ORR pursuant to 45 C.F.R. § 155.221(b)(4) and (f).

ii. Auditor Independence and Objectivity

An EDE Entity's Auditor must remain independent and objective throughout the audit process for both audits. 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 EDE environment and the determination of security and privacy control effectiveness or business requirement compliance. The Auditor's role is to provide an independent assessment of the compliance of the EDE Entity's EDE environment and to maintain the integrity of the audit process. Upon submission of the audit, Auditors 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.

VI. Business Audit Requirements and Scope

An Auditor will complete a business requirements audit to ensure the prospective EDE Entity (including a prospective phase change EDE Entity seeking to change phases or an upstream EDE Entity that has implemented one or more of the business requirements in Exhibit 2) has complied with applicable requirements. A prospective EDE Entity must submit the resulting business requirements audit package to CMS. The Auditor may define its own methodology to conduct the business requirements audit within the parameters defined in Exhibit 2, which summarizes the review areas and review standards for the business requirements audit.

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

Exhibit 2: Business Requirements

Review Category	Requirement and Audit Standard
Consumer Identity Proofing Implementation	▪ *Requirement*: The EDE Entity must conduct identity proofing (ID proofing) for Consumers entering the EDE pathway for enrollments through both Consumer and in-person Agent and Broker pathways.[61] In the Consumer pathway, the EDE Entity must conduct ID proofing prior to calling the Person Search API[62]. If an EDE Entity is unable to complete ID proofing of the Consumer, the EDE Entity may either direct the Consumer to the classic DE (i.e., double-redirect) pathway, an Agent/Broker, or to the Exchange (HealthCare.gov or the Exchange Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]). If an Agent or Broker is assisting the Consumer through the in-person Agent and Broker pathway, the EDE Entity must conduct ID proofing prior to submitting the application. – Remote ID Proofing/Fraud Solutions Archive Reporting Services (RIDP/FARS) or Third-Party ID Proofing Service: CMS will make the Exchange RIDP and FARS services available for the EDE Entity to use when remote ID proofing consumers for the Consumer pathway (i.e., when a consumer is interacting directly with the EDE environment without the assistance of an individual agent or broker). If an EDE Entity uses the Exchange RIDP service, it must use the RIDP service only after confirming the Consumer is seeking coverage in a state supported by the Exchange/Federal Platform, and only after confirming the consumer is eligible for the EDE Entity's chosen phase. However, CMS does not require that EDE Entities use the Exchange RIDP and FARS services, specifically, to complete ID proofing. An EDE Entity may instead opt to use a third-party ID proofing service for ID proofing in the consumer pathway. If an EDE Entity uses a third-party identity proofing service, the service must be Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS)-approved, and the EDE Entity must be able to produce documentary evidence that each Applicant has been successfully ID proofed. Documentation related to a third-party service could be requested in an audit or investigation by CMS (or its designee), pursuant to the EDE Business Agreement. Applicants do not need to be ID proofed on subsequent interactions with the EDE Entity if the Applicant creates an account (i.e., username and password) on the EDE Entity's website, and the EDE Entity tracks that ID proofing has occurred when the Applicant's account was created. – Manual ID Proofing in the In-Person Agent and Broker Pathway: EDE Entities may also offer a manual ID proofing process. Consumers being ID proofed in the in-person Agent and Broker pathway (i.e., when an Agent or Broker is working with a consumer and conducting ID proofing in-person, rather than remotely) must be ID proofed following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE (https://zone.cms.gov/document/api-information).

[61] Consumer pathway means the workflow, UI, and accompanying APIs for an EDE environment that is intended for use by a Consumer to complete an eligibility application and enrollment. Agent and Broker pathway means the workflow, UI, and accompanying APIs for an EDE environment that is intended for use by an Agent or Broker to assist a consumer with completing an eligibility application and enrollment.

[62] As described in the EDE API Companion Guide, for the consumer flow, the Person Search API can only be used as a back-end service. Accordingly, EDE Entities must restrict consumers from providing direct inputs into a Person Search UI component. EDE Entities must use the demographic information collected during ID proofing to search for a consumer's application(s) in the EDE consumer flow. The API Companion Guide is available at the following link: https://zone.cms.gov/document/api-information.

Review Category	Requirement and Audit Standard
Consumer Identity Proofing Implementation (continued)	– For the Consumer pathway, the EDE Entity must provide the User ID of the requester in the header for each EDE API call. For the Consumer pathway, the User ID should be the User ID for the Consumer's account on the EDE Entity's site, or some other distinct identifier the EDE Entity assigns to the Consumer. – Additionally, if an EDE Entity is using the Fetch Eligibility API, the same User ID requirements apply. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID. ▪ Review Standard: – EDE Entity's process for ID proofing a Consumer prior to submitting a Consumer's application to the Exchange. – If an EDE Entity uses the Exchange RIDP service, the Auditor must verify that the EDE Entity has successfully passed testing with the Hub.[63] – If an EDE Entity uses a third-party ID proofing service, the Auditor must evaluate and certify the following: o The ID proofing service is FICAM TFS-approved, and o The EDE Entity has implemented the service correctly. – If an EDE Entity offers a Manual ID proofing option for an in-person Agent and Broker pathway, the Auditor must verify that the EDE Entity requires Agents and Brokers to ID proof consumers as described in the "Acceptable Documentation for Identity Proofing" document. – EDE Entity's inclusion of the appropriate Consumer User ID fields in the EDE and Fetch Eligibility API calls.

[63] RIDP/FARS testing requirements for the Hub can be found at the following link on CMS zONE: https://zone.cms.gov/document/api-information.

Review Category	Requirement and Audit Standard
Agent and Broker Identity Proofing Verification	▪ *Requirement:* If an EDE Entity is implementing an Agent and Broker pathway for its EDE environment, the EDE Entity must implement Agent and Broker ID proofing verification procedures that consist of the following requirements: – EDE Entity must integrate with IDM-Okta[64] and provide the User ID of the requester and IDM-Okta token in the header for each EDE API call. For Agents and Brokers, the User ID must exactly match the Exchange User ID (i.e. the Agent's or Broker's portal.cms.gov User ID) for the Agent or Broker, or the request will fail Exchange User ID validation. o The same User ID requirements apply to the Fetch Eligibility and Submit Enrollment APIs. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID. – EDE Entity must ID proof all Agents and Brokers prior to allowing the Agents and Brokers to use its EDE environment. EDE Entity may conduct ID proofing in one of the following ways: o Use the Exchange-provided RIDP/FARS APIs to remotely ID proof Agents and Brokers; OR o Manually ID proof Agents and Brokers following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE EDE webpage (https://zone.cms.gov/document/api-information). o EDE Entities are permitted to use manual ID proofing as an alternative for Agents and Brokers that cannot be ID proofed via the RIDP/FARS services. – EDE Entity must validate an Agent's or Broker's National Producer Number (NPN) using the National Insurance Producer Registry (https://www.nipr.com) prior to allowing the Agent or Broker to use its EDE environment. – EDE Entity must systematically provide an Agent and Broker ID proofing process—that meets all of the requirements defined here—that applies to all downstream Agents and Brokers of the primary EDE Entity. – Additionally, all Agent and Broker users of an upstream EDE Entity's EDE website (hosted by a primary EDE Entity) must be ID proofed consistent with these requirements. The primary EDE Entity may provide one centralized ID proofing approach for any Agents and Brokers that will use the primary EDE Entity's EDE environment (including when utilized by upstream EDE Entities and their downstream Agents and Brokers).

[64] For instructions on how to integrate with IDM-Okta, see the Change Request #55 Integration Manual (IDM Integration), available at: https://zone.cms.gov/document/business-audit and Hub Onboarding Form, available at: https://zone.cms.gov/document/hub-onboarding-form.

Review Category	Requirement and Audit Standard
Agent and Broker Identity Proofing Verification (continued)	○ Alternatively, the upstream EDE Entity may conduct its own ID proofing process of its downstream Agents and Brokers consistent with these requirements. The upstream EDE Entity must provide the information for Agents and Brokers that have passed and failed ID proofing to the primary EDE Entity using a secure data transfer. If an upstream EDE Entity wants to pursue this flexibility, its ID proofing process must be audited by an Auditor consistent with these standards and the arrangement will be considered a hybrid arrangement. – Note: If a primary EDE Entity does not provide a centralized process for ID proofing an upstream EDE Entity's downstream Agent and Broker and if the primary EDE Entity intends to provide the EDE environment to upstream EDE Entities, the upstream EDE Entities will be required to provide documentation of an Auditor's evaluation of its ID proofing approach consistent with these standards. This process must be categorized as an EDE Entity-initiated Change Request (Section XI.A, EDE Entity-initiated Change Requests) if it occurs after the primary EDE Entity's initial audit submission and the arrangement with the upstream EDE Entity will be considered a hybrid arrangement. – All Agents and Brokers that will use EDE must be ID proofed consistent with these standards. This includes downstream Agents and Brokers of primary EDE Entities and upstream EDE Entities. The Auditor must evaluate the primary EDE Entity's centralized implementation for ID proofing (if applicable) or the upstream EDE Entity's implementation for ID proofing (if applicable). – EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3. ▪ *Review Standard:* The Auditor must verify and certify the following: – EDE Entity's inclusion of the appropriate Agent and Broker User ID and IDM-Okta token fields in the EDE and Fetch Eligibility and Submit Enrollment API calls. – EDE Entity's process for ID proofing an Agent or Broker prior to allowing an Agent or Broker to use its EDE environment. – EDE Entity's process for validating an Agent's or Broker's NPN using the National Insurance Producer Registry prior to allowing an Agent or Broker to use its EDE environment. – EDE Entity's process for systematically providing an Agent and Broker ID proofing approach for all downstream Agents and Brokers of the EDE Entity and, if applicable, any upstream EDE Entities. – If the primary EDE Entity has not provided a centralized ID proofing approach to an upstream EDE Entity, primary EDE Entity's process for verifying that an upstream EDE Entity has conducted appropriate ID proofing, consistent with this requirement, for all of the upstream EDE Entity's downstream Agents and Brokers prior to those Agents and Brokers being able to use the primary EDE Entity's EDE environment.
Phase-dependent Screener Questions (EDE Phase 2 Entities Only)	▪ *Requirement:* An EDE Entity that implements EDE Phase 2 must implement screening questions to identify Consumers whose eligibility circumstances the EDE Entity is unable to support consistent with the eligibility scenarios supported by the EDE Entity's selected EDE phase. These phase-dependent screener questions must be located at the beginning of the EDE application, but may follow the QHP plan compare experience. For those Consumers who won't be able to apply through scenarios covered by the EDE phase that the EDE Entity implements, the EDE Entity must either route the Consumer to the classic DE double-redirect pathway or direct the Consumer to the Exchange by providing the following options: HealthCare.gov or the Exchange Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]. ▪ *Review Standard*: The Auditor must verify the following: – The EDE Entity has implemented screening questions—consistent with the requirements in the Exchange Application UI Principles document and Application UI Toolkit—to identify Consumers with eligibility scenarios not supported by the EDE Entity's EDE environment and selected EDE phase. – The EDE Entity's EDE environment facilitates moving Consumers to one of the alternative enrollment pathways described immediately above.

Review Category	Requirement and Audit Standard
Accurate and Streamlined Eligibility Application User Interface (UI)	▪ *Requirement:* EDE Entities using the EDE pathway must support all application scenarios outlined in EDE Entity's selected EDE phase. The EDE Entity must adhere to the guidelines set forth in the FFE Application UI Principles document when implementing the application. EDE Entities can access the FFE Application UI Principles document on CMS zONE (https://zone.cms.gov/document/eligibility-enrollment-information). Auditors will need to access the FFE Application UI Principles document to conduct the audit. – As explained in the FFE Application UI Principles document, the EDE Entity must implement the application in accordance with the Exchange requirements. For each supported eligibility scenario, the EDE Entity must display all appropriate eligibility questions and answers, including all questions designated as optional. (Note: These questions are optional for the Consumer to answer, but are not optional for EDE Entities to implement.) The FFE Application UI Principles document and Application UI Toolkit define appropriate flexibility EDE Entities may implement with respect to question wording, question order or structure, format of answer choices (e.g., drop-down lists, radio buttons), and integrated help information (e.g., tool tips, URLs, help boxes). In most cases, answer choices, question logic (e.g., connections between related questions), and disclaimers (e.g., APTC attestation) must be identical to those of the Exchange. o Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this exceeds the scope of the test cases in the Eligibility Results Toolkits. – EDE Entities will also need to plan their application's back-end data structure to ensure that attestations can be successfully submitted to Standalone Eligibility Service (SES) APIs at appropriate intervals within the application process and that the EDE Entity can process responses from SES and integrate them into the UI question flow logic, which is dynamic for an individual Consumer based on his or her responses. The EDE Entity will need to ensure that sufficient, non-contradictory information is collected and stored such that accurate eligibility results will be reached without any validation errors. ▪ *Review Standard*: The Auditor must review and certify the following: – The FFE Application UI has been implemented in EDE Entity's environment in accordance with the Exchange Application UI Principles document. – The FFE Application UI displays all appropriate eligibility questions and answers from the Application UI Toolkit, including any questions designated as optional. – The Auditor will review the application for each supported eligibility scenario under the phase the EDE Entity has implemented to confirm that the application has been implemented in accordance with the FFE Application UI Principles document and Application UI Toolkit. The Auditor will document this compliance in the Application UI Toolkit. o Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this exceeds the scope of the test cases in the Eligibility Results Toolkits. – If EDE Entity has implemented Phase 2, the Auditor will confirm that the UI includes a disclaimer stating that the environment does not support all application scenarios, and identifying which scenarios are and are not supported. The disclaimer should direct the Consumer to alternative pathways, such as the classic DE double-redirect pathway or direct the Consumer to the Exchange (HealthCare.gov or the Exchange Call Center at 1-800-318-2596 (TTY: 1-855-889-4325)). This requirement is included in the Communications Toolkit.

Review Category	Requirement and Audit Standard
Post-eligibility Application Communications	▪ *Requirement*: The EDE environment must display high-level eligibility results, next steps for enrollment, and information about each Applicant's insurance affordability program eligibility (e.g., APTC, CSR, Medicaid, and/or CHIP eligibility), Data Matching Issues (DMIs), special enrollment periods (SEPs), SEP Verification Issues (SVIs), and enrollment steps in a clear, comprehensive and Consumer-friendly way. Generally, CMS's Communications Toolkit constitutes the minimum post-eligibility application communications requirements that an EDE Entity must provide to users of the EDE environment; CMS does not intend for the Communications Toolkit requirements to imply that EDE Entities are prohibited from providing additional communications or functionality, consistent with applicable requirements. – EDE Entity must provide Consumers with required UI messaging tied to API functionality and responses as provided in the EDE API Companion Guide[65]. – EDE Entity must provide Consumers with the CMS-provided Eligibility Determination Notices (EDNs) generated by the Exchange any time it submits or updates an application pursuant to requirements provided by CMS in the Communications Toolkit.

[65] The API Companion Guide is available on CMS zONE at the following link: https://zone.cms.gov/document/api-information.

Review Category	Requirement and Audit Standard
Post-eligibility Application Communications (continued)	– EDE Entity must provide the EDN in a downloadable format at the time the Consumer's application is submitted or updated and must have a process for providing access to the Consumer's most recent EDN via the API as well as providing access to the Consumer's historical notices—accessed via the Notice Retrieval API by the EDE Entity's EDE environment—within the UI. The UI requirements related to accessibility of a Consumer's EDN are set forth in the Communications Toolkit. – EDE Entities are not required to store notices downloaded from the Exchange. EDE Entities must use the Metadata Search API and the Notice Retrieval API to generate the most recent Exchange notices when Consumers act to view/download notices consistent with the Communications Toolkit. EDE Entities must also provide access to view/download historical notices in their UIs. – EDE Entity must provide and communicate status updates and access to information for Consumers to manage their applications and coverage. These communications include, but are not limited to, status of DMIs and SVIs, enrollment periods (e.g., SEP eligibility and the OEP), providing and communicating about new notices generated by the Exchange, application and enrollment status, and supporting document upload for DMIs and SVIs. This requirement is detailed in the Communications Toolkit. – EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI (e.g., an account management hub for managing all application- and enrollment-related actions). – For any Consumers enrolled, including via the Agent and Broker pathway, the EDE Entity must provide critical communications to Consumers notifying them of the availability of Exchange-generated EDNs, critical communications that the Consumer will no longer receive from the Exchange (i.e., if the EDE Entity has implemented and been approved by CMS to assume responsibility for those communications), and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer's application or enrollment status. – All EDE Entities, regardless of phase, must provide consumers with status updates and document upload capabilities for all DMIs and SVIs. Even if an EDE Entity's chosen eligibility application phase does not support the questions necessary to reach a certain DMI or SVI, the post-application and post-enrollment functionality must support any consumer with any DMI or SVI; post-application and post-enrollment DMI and SVI management is not dependent on the EDE Entity's chosen eligibility application phase. ▪ *Review Standard*: The Auditor must verify and certify the following: – The EDE Entity's EDE environment is compliant with the requirements contained in the Communications Toolkit and API Companion Guide. – The EDE Entity's EDE environment notifies Consumers of their eligibility results prior to QHP enrollment, including when submitting a CiC in the environment. For example, if a Consumer's APTC or CSR eligibility changes, EDE Entity must notify the Consumer of the change and allow the Consumer to modify his or her QHP selection (if SEP-eligible) or APTC allocation accordingly. – EDE Entity must have a process for providing Consumers with a downloadable EDN in its EDE environment and for providing access to a current EDN via the API. EDE Entity must share required eligibility information that is specified by CMS in the Communications Toolkit. – The Auditor must verify that EDE Entity's EDE environment is providing status updates and ongoing communications to Consumers according to CMS requirements in the Communications Toolkit as it relates to the status of their application, eligibility, enrollment, notices, and action items the Consumer needs to take. – The EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI. – The EDE Entity must have a means for providing critical communications to the Consumer consistent with the standards above. – The EDE Entity must support all DMIs and SVIs in its post-eligibility application and post-enrollment functionality.

Review Category	Requirement and Audit Standard
Accurate Information about the Exchange and Consumer Communications	▪ *Requirement:* EDE Entity must provide Consumers with CMS-provided language informing and educating the Consumers about the Exchanges and HealthCare.gov and Exchange-branded communications Consumers may receive with important action items. CMS defines these requirements in the Communications Toolkit. ▪ *Review Standard:* The Auditor must verify and certify that the EDE Entity's EDE environment includes all required language, content, and disclaimers provided by CMS in accordance with the standards stated in guidance and the Communications Toolkit.
Documentation of Interactions with Consumer Applications or the Exchange	▪ *Requirement:* EDE Entity must implement and maintain tracking functionality on its EDE environment to track Agent, Broker, and Consumer interactions, as applicable, with Consumer applications using a unique identifier for each individual, as well as an individual's interactions with the Exchanges (e.g., application; enrollment; and handling of action items, such as uploading documents to resolve a DMI). This requirement also applies to any actions taken by a downstream Agent or Broker,[66] as well as the upstream EDE Entity users, of a primary EDE Entity's EDE environment. ▪ *Review Standard:* The Auditor must verify EDE Entity's process for determining and tracking when an upstream EDE Entity, downstream Agent or Broker, and Consumer has interacted with a Consumer application or taken actions utilizing the EDE environment or EDE APIs. The Auditor must verify and certify the following: – The EDE Entity's environment tracks, at a minimum, the interactions of upstream EDE Entities, downstream Agents or Brokers, and Consumers with a Consumer's account, records, application, or enrollment information utilizing the EDE environment or EDE APIs. – The EDE Entity's environment tracks when an upstream Entity, downstream Agent or Broker, or Consumer views a Consumer's record, enrollment information, or application information utilizing the EDE environment or EDE APIs. – The EDE Entity's environment uses unique identifiers to track and document activities by Consumers, downstream Agents and Brokers, and upstream EDE Entities using the EDE environment. – The EDE Entity's environment tracks interactions with the EDE suite of APIs by an upstream EDE Entity, a downstream Agent or Broker, or Consumer. – The EDE Entity's environment stores this information for 10 years.

[66] Note: References to downstream Agents and Brokers include downstream Agents and Brokers of either the primary EDE Entity or an upstream EDE Entity.

Review Category	Requirement and Audit Standard
Eligibility Results Testing and SES Testing	▪ *Requirement*: EDE Entity must submit accurate applications through its EDE environment that result in accurate and consistent eligibility determinations for the supported eligibility scenarios covered by EDE Entity's chosen EDE phase. – The business requirements audit package must include testing results in the designated Exchange EDE testing environment. CMS has provided a set of Eligibility Results Toolkits with the eligibility testing scenarios on CMS zONE https://zone.cms.gov/document/business-audit). ▪ *Review Standard*: The Auditor must verify and certify the following: – The Auditor was able to successfully complete a series of test eligibility scenarios in the EDE Entity's EDE environment implementation using the Eligibility Results Toolkits. For example, these scenarios may include Medicaid and CHIP eligibility determinations, and different combinations of eligibility determinations for APTC and CSRs. Note: These scenarios do not test, and are not expected to test, every possible question in the Application UI flow for an EDE Entity's selected phase. In addition to reviewing the eligibility results test cases, the Auditor must review the Application UI for compliance as defined above. – The Auditor must test each scenario and verify that the eligibility results and the eligibility process were identical to the expected results and process. The Auditor must provide CMS confirmation that each relevant eligibility testing scenario was successful, that the expected results were received, and must submit the required proof, as defined in the Eligibility Results Toolkits. This will include screenshots, EDNs, and the raw JSON from the Get App API response for the application version used to complete the scenario. Note: EDNs and raw JSONs are required for all required toolkit scenarios; however, screenshots are only required for the highest phase an entity is submitting (for example, a prospective phase 3 EDE Entity must submit screenshots for the Phase 3 Eligibility Results Toolkit only, but must submit EDNs and raw JSONs for applicable Phase 2 and Phase 3 toolkit scenarios).
API Functional Integration Requirements	▪ *Requirement*: EDE Entity must implement the EDE API suite and corresponding UI functionality in accordance with the API specifications and EDE API Companion Guide provided by CMS. The EDE API specifications and EDE API Companion Guide are available on CMS zONE (https://zone.cms.gov/document/api-information). ▪ *Review Standard:* The Auditor must complete the set of test scenarios as outlined in the API Functional Integration Toolkit to confirm that the EDE Entity's API and corresponding UI integration performs the appropriate functions when completing the various EDE tasks. For example, the Auditor may have to complete a scenario to verify that a Consumer or Agent and Broker is able to view any SVIs or DMIs that may exist for a consumer, and confirm that the Consumer or Agent and Broker has the ability to upload documents to resolve any SVIs or DMIs. Some of the test cases require that the Auditor and EDE Entity request CMS to process adjudication actions; the Auditor cannot mark these particular test cases as compliant until evaluating whether the expected outcome occurred after CMS takes the requested action. The Auditor will also need to be aware of the following requirements related to the test scenarios: – Test scenarios in the API Functionality Integration Toolkit must be completed for both the Consumer pathway and the Agent and Broker pathway if an EDE Entity is pursuing approval to use both pathways. – The API Functional Integration Toolkit includes a "Required Evidence" column, Column H, on the "Test Cases" tab. Auditors will need to submit the applicable "Required Evidence," including the complete header and body for each required API request and response, as part of the audit submission.
Application UI Validation	▪ *Requirement:* EDE Entity must implement CMS-defined validation requirements within the application. The validation requirements prevent EDE Entity from submitting incorrect data to the Exchange. ▪ *Review Standard:* The Auditor must confirm that EDE Entity has implemented the appropriate application field-level validation requirements consistent with CMS requirements. These field-level validation requirements are documented in the FFE Application UI Principles document.

Review Category	Requirement and Audit Standard
Section 508-compliant UI	▪ *Requirement:* Pursuant to 45 C.F.R. § 155.220(c)(3)(ii)(D) (citing 45 C.F.R. §§ 155.230 and 155.260(b)) and 45 C.F.R. § 156.265(b)(3)(iii) (citing 45 C.F.R. §§ 155.230 and 155.260(b)), web-brokers and QHP issuers participating in DE, including all EDE Entities, must implement an eligibility application UI that is Section 508 compliant. A Section 508-compliant application must meet the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)). ▪ *Review Standard*: The Auditor must confirm that EDE Entity's application UI meets the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)). The Auditor must verify and certify the following: – Within the Business Requirements Audit Report Template, the Auditor must confirm that the EDE Entity's application UI is Section 508 compliant. No specific report or supplemental documentation is required. – The Auditor may review results produced by a 508 compliance testing tool. If an EDE Entity uses a 508 compliance testing tool to verify that its application UI is 508 compliant, its Auditor must, at a minimum, review the results produced by the testing tool and document any non-compliance, as well as any mitigation or remediation to address the non-compliance. It is not sufficient for an Auditor to state that an EDE Entity complies with this requirement by confirming that the EDE Entity utilized a 508 compliance testing tool.
Non-English-language Version of the Application UI and Communi-cation Materials	▪ *Requirement*: In accordance with 45 C.F.R. § 155.205(c)(2)(iv)(B) and (C), QHP issuers and web-brokers, including those that are EDE Entities, must translate applicable website content (e.g., the application UI) on Consumer-facing websites into any non-English language that is spoken by a limited English proficient (LEP) population that reaches ten (10) percent or more of the population of the relevant state, as determined in current guidance published by the Secretary of HHS.[67] EDE Entities must also translate communications informing Consumers of the availability of Exchange-generated EDNs; critical communications that the Consumer will no longer receive from the Exchange (i.e., if the EDE Entity has implemented and been approved by CMS to assume responsibility for those communications); and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer's use of its EDE environment into any non-English language that is spoken by an LEP population that reaches ten (10) percent or more of the population of the relevant state, as determined in guidance published by the Secretary of HHS.[68] ▪ *Review Standard*: The Auditor must verify and certify the following: – The Auditor must confirm that the non-English-language version of the application UI and associated critical communications are compliant with the Exchange requirements, including the Application UI Toolkit and Communications Toolkit. – The Auditor must verify that the application UI has the same meaning as its English-language version. – The Auditor must also verify that EDE Entity has met all EDE communications translation requirements released by CMS in the Communications Toolkit. – The Auditor must document compliance with this requirement within the Business Requirements Audit Report Template, the Application UI Toolkit, and the Communications Toolkit. In the toolkits, the Auditor can add additional columns for the Auditor compliance findings fields (yellow-shaded columns) or complete the Spanish audit in a second copy of each of the two toolkits.

[67] Guidance and Population Data for Exchanges, Qualified Health Plan Issuers, and Web-Brokers to Ensure Meaningful Access by Limited-English Proficient Speakers Under 45 CFR §155.205(c) and §156.250 (March 30, 2016) https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Language-access-guidance.pdf and "Appendix A- Top 15 Non-English Languages by State" https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508_update12-20-16.pdf.

[68] *Frequently Asked Questions (FAQs) Regarding Spanish Translation and Audit Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with Federally-facilitated Exchanges (FFEs)* (June 20, 2018) provides further information regarding translation and audit requirements: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-Spanish-Translation-and-Audit-Requirements.PDF.

Review Category	Requirement and Audit Standard
EDE Change Management Process	▪ *Requirement*: EDE Entity must develop and consistently implement processes for managing changes to the EDE environment relevant to the business requirements audit requirements. This requirement does not replace the evaluation necessary for relevant privacy and security controls. At a minimum, the EDE Entity's change management plan must include the following elements: – A process that incorporates all elements of the Change Notification SOP as referenced in Section XI.A.i, EDE Entity-initiated Change Request Process; – All application and business audit-related changes are thoroughly defined and evaluated prior to implementation, including the potential effect on other aspects of the EDE end-user experience; – A process for defining regression testing scope and developing or identifying applicable testing scenarios; – A process for conducting regression testing; – A process for identifying and correcting errors discovered through regression testing and re-testing the correction; – A process for maintaining separate testing environments and defining the purposes and releases for each environment; – The change management process must be maintained in writing and relevant individuals must be informed on the change management process and on any updates to the process; and – The change management process must include a process, if applicable, for an EDE Entity to update the non-English-language version of the application UI and communication materials for any changes to the application UI or communication materials in the English-language version of the EDE environment. – A process for assessing Section 508 compliance for changes to the EDE Environment consistent with Exhibit 2: Business Requirements. ▪ *Review Standard*: The Auditor must evaluate the EDE Entity's change management plan for compliance with the elements and criteria defined above.
Health Reimbursement Arrangement (HRA) Offer Required UI Messaging	▪ *Requirement*: Phase 3 EDE Entities, Phase 2 EDE Entities that optionally implement full HRA functionality, and EDE Entities that also offer a classic DE pathway, must implement required UI messaging for qualified individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the qualified individuals consistent with CMS guidance. Required UI messaging for various scenarios are detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.[69] ▪ *Review Standard*: The Auditor must review the EDE Entity's HRA offer implementation to confirm that the required UI messaging content is displayed for each of the relevant scenarios detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.

A. Application Phase Options

CMS is offering the option of implementing one of two phases of the eligibility application when using the EDE pathway. An EDE Entity may choose to implement Phase 2 or 3[70] (described further below) for Year 7 of EDE. A prospective EDE Entity must commit to a phase and complete the phase implementation prior to initiating its audit because the audit must evaluate the compliance of the prospective EDE Entity's EDE environment with the requirements of the applicable phase. It is imperative that EDE Entities carefully evaluate the available application phases and select appropriate phases that they can reasonably implement within the available time before the next audit submission window, as well as their organization's business needs, resources, expertise, and capacity. Once an Entity starts developing for its selected phase, it is recommended that the Entity not seek to change phases until the Entity is approved to go live

[69] The document *FFEs DE API for Web-brokers/Issuers Technical Specifications (Direct Enrollment API Specs)* is available on CMS zONE at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

[70] As described in this section, for Year 7 of EDE, CMS will no longer permit primary EDE Entities to implement eligibility application Phase 1.

with its originally selected phase. If an Entity has not completed its build, changing phases may require the Entity to modify elements of its implementation depending on how much of the system it has already built. Similarly, once an Entity begins its audit, it may need to re-audit elements of its implementation depending on the extent of the changes and how much of the system has already been audited. After conducting and submitting audits, Entities must not modify their EDE environments to change phases without consulting CMS and, if an Entity chooses to move forward with a phase change in this situation, it must follow the processes defined below in Section XI, Processes for Changes to an Audited or Approved EDE Environment, which includes conducting an additional business requirements audit as a prospective phase change EDE Entity.

EDE Entities that implement Phase 2 must implement screening questions to redirect consumers whose eligibility circumstances the EDE Entities are unable to support to other supported application and enrollment channels. Please refer to Exhibit 3 for more information on the screening scenarios and Exhibit 2 for information on the screening question and communication requirements.

Exhibit 3: End-state Application Phases

End State Phases	Description	Benefits
Phase 2: Host Expanded Simplified Application + EDE API Suite	EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following: ▪ Application filer (and others on application, if applicable) resides in the application state and all dependents have the same permanent address, if applicable ▪ Application filer plans to file a federal income tax return for the coverage year; if married plans to file a joint federal income tax return with spouse ▪ Application filer (and spouse, if applicable) is not responsible for a child 18 or younger who lives with the Application filer but is not on his/her federal income tax return ▪ No household members are full-time students aged 18-22 ▪ No household member is pregnant ▪ All applicants are U.S. citizens ▪ All applicants can enter Social Security Numbers (SSNs) ▪ No applicants are applying under a name different than the one on his/her Social Security cards ▪ No applicants were born outside of the U.S. and became naturalized or derived U.S. citizens ▪ No applicants are currently incarcerated (detained or jailed) ▪ No household members are American Indian or Alaska Native ▪ No applicants are offered health coverage through a job or COBRA ▪ No applicants are offered an individual coverage health reimbursement arrangement (HRA) or qualified small employer health reimbursement arrangement (QSEHRA) ▪ No applicants were in foster care at age 18 and are currently 25 or younger ▪ All dependents are claimed on the Application filer's federal income tax return for the coverage year ▪ All dependents are the Application filer's children who are single (not married) and 25 or younger ▪ No dependents are stepchildren or grandchildren ▪ No dependents live with a parent who is not on the Application filer's federal income tax return ▪ Full-time student ▪ Pregnant application members ▪ Non-U.S. citizens ▪ Naturalized U.S. citizens ▪ Application members who do not provide an SSN ▪ Application members with a different name than the one on their SSN cards ▪ Incarcerated application members ▪ Application members who previously were in foster care ▪ Stepchildren	Lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.

End State Phases	Description	Benefits
Phase 3: Host Complete Application + EDE API Suite	EDE Entity hosts an application that supports all application scenarios (equivalent to existing HealthCare.gov): ▪ All scenarios covered in Phase 2 ▪ American Indian and Alaskan Native household members ▪ Application members with differing home addresses or residing in a state separate from where they are applying for coverage ▪ Application members with no home address ▪ Application members not planning to file a tax return ▪ Married application members not filing jointly ▪ Application members responsible for a child age 18 or younger who lives with them, but is not included on the Application filer's federal income tax return (parent/caretaker relative questions) ▪ Application members offered coverage through their job, someone else's job, or COBRA ▪ Application members with dependent children who are over age 25 or who are married ▪ Application members with dependent children living with a parent not on their federal income tax return ▪ Dependents who are not sons/daughters ▪ Applicants who are offered an individual coverage HRA or QSEHRA	Highest level of effort to implement and audit. EDE Entity would provide and service the full range of consumer scenarios. Additionally, the EDE Entity would no longer need to redirect consumers to alternative pathways for complex eligibility scenarios. Please note that the implementation of Phase 3 is comparatively more complex than Phase 2 and may require more time to implement, audit, and approve.

i. Limited Applicability of Eligibility Application Phase Selection on EDE Requirements

A primary EDE Entity's selected eligibility application phase only modifies the requirements of the eligibility application implementation. In general, all primary EDE Entities, regardless of the eligibility application phase chosen, must implement all EDE requirements for primary EDE Entities, unless stated otherwise in these guidelines, including requirements that may relate to eligibility application questions or results (e.g., post-application support for DMIs related to phase-specific eligibility application questions).

All EDE Entities, regardless of the phase chosen, are required to support consumer-reported changes in circumstances (CiCs) and special enrollment periods (SEPs) during and outside of the OEP. In addition, they are required to support re-enrollment application activities for any such actions that fall within the scenarios supported by the EDE Entity's chosen end-state phase. Furthermore, all EDE Entities, regardless of the phase chosen, must support households that wish to enroll in more than one enrollment group. Consistent with the general expectation that EDE requirements and functionalities be implemented for and provided to all users of an EDE environment, primary EDE Entities must provide the functionalities described in this paragraph for all users of the primary EDE Entity's EDE environment, including any upstream EDE Entities and their users. Exhibit 3 describes each of the two end-state application phases and explains their benefits.

In addition to the Application UI, EDE Entities are required to provide account management functions for consumers. EDE Entities must also provide required information in the UI and via email related to a consumer's application and enrollment status. These communications include, but are not limited to, providing status updates on the application and enrollment; providing information and updates on DMIs and SVIs, enrollment periods, and notices that are generated

by the Exchange; facilitating document uploads for DMIs and SVIs; and updating and reporting changes to application and enrollment information. Generally, the account management and communications requirements are not phase-specific requirements. With the exception of the phase-specific disclaimer requirement described in the Communications Toolkit, EDE Entities must implement these communications and account management requirements and provide the relevant functionality and communications to users of the EDE environment regardless of an Entity's selected end-state application phase. To review more detailed descriptions of communications requirements, please refer to the most recent version of the Communications Toolkit, which is available on CMS zONE.[71]

ii. Limitations on Eligibility Application Phases 1 and 2 for the EDE Year 7 Audit Submission Window and Beyond

Beginning with these guidelines and Year 7 of EDE, CMS will no longer accept eligibility application Phase 1 audit submissions from primary EDE Entities. CMS will also require all existing primary EDE Entities approved to use eligibility application Phase 2 to transition to eligibility application Phase 3. Primary EDE Entities that CMS has approved to use eligibility application Phase 2 prior to the audit submission window for Year 7 of EDE must implement eligibility application Phase 3 and submit a complete phase change audit submission for eligibility application Phase 3 no later than 3 a.m. ET on July 1, 2026, consistent with Section XI.A.ii.

If a primary EDE Entity currently approved for eligibility application Phase 2 fails to submit a phase change audit submission by that deadline, CMS will not renew the primary EDE Entity's EDE Business Agreement and Interconnection Security Agreement prior to the Plan Year 2027 Open Enrollment Period and will terminate the primary EDE Entity's access to the Data Services Hub in production.

Similarly, CMS will require that all prospective primary EDE Entities that implement eligibility application Phase 2 must submit a complete phase change audit submission for eligibility application Phase 3 no later than the second audit submission window that follows CMS's approval for the EDE Entity to go live with eligibility application Phase 2. Prospective primary EDE Entities that submit an initial business audit for eligibility application Phase 2 in the Year 7 audit submission window (or a subsequent audit submission window) must implement eligibility application Phase 3 and submit a complete phase change audit, consistent with Section X.C, for eligibility application Phase 3 within two (2) audit submission windows after approval to go live with Phase 2. For example, a prospective EDE Entity who is approved to go live with Phase 2 in calendar year 2026 must implement Phase 3 and submit a phase change audit during either the calendar year 2027 or calendar year 2028 audit submission window. If a primary EDE Entity approved for eligibility application Phase 2 fails to submit a phase change audit submission by that second audit submission window, CMS will not renew the primary EDE Entity's EDE Business Agreement and Interconnection Security Agreement prior to the Open Enrollment Period that follows the second audit submission window and will terminate the primary EDE Entity's access to the Data Services Hub in production.

[71] The Communications Toolkit is stored within the EDE Business Requirements Audit and Report Template and Toolkits file available at the following link: https://zone.cms.gov/document/business-audit.

B. Audit Documentation

i. Required Business Requirements Audit Documentation

Exhibit 4 contains the required information that prospective EDE Entities (including a prospective phase change EDE Entity) must submit to CMS as part of the business requirements audit to be approved to participate in EDE. CMS encourages prospective EDE Entities to use this table as a checklist to ensure they have met all requirements. Note: CMS may require prospective EDE Entities and/or their Auditors to submit additional documents and information at CMS's discretion.

Exhibit 4: Required Information for Business Requirements Audit

Document	Description	Submission Requirements	Entity Responsible	Deadline
Notice of Intent to Participate and Auditor Confirmation	▪ Once the prospective primary and prospective phase change EDE Entity has a confirmed Auditor(s) who will be completing its audit(s), it must notify CMS that it intends to apply to use the EDE pathway prior to initiating the audit. The email must include the following: – Prospective EDE Entity Name – Auditor Name(s) and Contact Information (Business Requirements and Privacy and Security, if different) – A copy of the executed contract with the Auditor(s) (pricing and proprietary information may be redacted) – EDE Phase (1, 2, or 3) – Prospective EDE Entity Primary Point of Contact (POC) name, email, and phone number. The Primary POC should be a person who is able to make decisions on behalf of the Entity. – Prospective EDE Entity Technical POC name, email, and phone number. The Technical POC should be a person who manages technical development. – Prospective EDE Entity Emergency POC name, email, and phone number. The Emergency POC should be a person who should be contacted in an emergency situation.[72] – CMS-issued Hub Partner ID	▪ The prospective primary and prospective phase change EDE Entity must email directenrollment@cms.hhs.gov ▪ Subject line should state: "Enhanced DE: Intent."	Prospective primary and prospective phase change EDE Entities Note: CMS is not collecting notices of intent from prospective upstream EDE Entities.	March 1, 2024

Document	Description	Submission Requirements	Entity Responsible	Deadline
***DE Entity Documentation Package*—Privacy Questionnaire (or attestation, if applicable, see Submission Requirements column)**	▪ CMS has provided the privacy questionnaire as part of the DE Entity Documentation Package available on CMS zONE. ▪ EDE Entity must populate the privacy questionnaire and return it to CMS for review.	▪ Submit via the DE/EDE Entity PME Site ▪ If an EDE Entity's responses to the privacy questionnaire are unchanged from the EDE Entity's last submission of a privacy questionnaire, the Entity may submit an attestation stating that the previously submitted questionnaire remains accurate. – The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents.	Prospective primary EDE Entities	Submit with audit submission

[72] CMS will send EDE related communications to the POCs listed in the EDE Entity's Notice of Intent to Participate. EDE Entities can change these POCs at any time by emailing directenrollment@cms.hhs.gov.

Document	Description	Submission Requirements	Entity Responsible	Deadline
***DE Entity Documentation Package*—Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements column)**	▪ Submit the URL and text of each privacy policy statement displayed on your website and your website's Terms of Service in a Microsoft Word document or a PDF. ▪ The privacy policy and terms of service must be submitted for any EDE Entity's website that is collecting consumer data as part of the EDE end-user experience.	▪ Submit via the DE/EDE Entity PME Site ▪ If an EDE Entity's privacy policy and Terms of Service remain unchanged from the EDE Entity's last submission of the privacy policy and Terms of Service, the Entity may submit an attestation stating that the previously submitted privacy policy and Terms of Service will remain unchanged. – The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents	Both prospective primary and prospective upstream EDE Entities	Prospective primary EDE Entities: Submit with audit submission. Prospective upstream EDE Entities: Submit after the prospective primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the PY 2024 DE Entity documentation package for prospective upstream EDE Entities, but to be reasonably certain a prospective upstream EDE Entity will be approved by November 1, 2024, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1, 2024 or as soon as feasible to allow time to review prior to activating their Partner IDs.
EDE Business Agreement	▪ EDE Entities must execute the EDE Business Agreement to use the EDE pathway. The agreement must identify the Entity's selected Auditor(s) (if applicable). ▪ CMS will countersign the EDE Business Agreement after CMS has reviewed and approved the EDE Entity's business requirements audit and the privacy and security audit.	▪ Submit via the DE/EDE Entity PME Site	Both prospective primary and prospective upstream EDE Entities	Prospective primary EDE Entities: Submit with audit submission. Prospective upstream EDE Entities: Submit after the prospective primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for prospective upstream EDE Entities, but to be reasonably certain a prospective upstream EDE Entity will be approved by November 1, 2024, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1, 2024 or as soon as feasible to allow time to review prior to activating their Partner IDs.

Document	Description	Submission Requirements	Entity Responsible	Deadline
***DE Entity Documentation Package*— Operational and Oversight Information**	▪ EDE Entities must submit the operational and oversight information to CMS to use the EDE pathway. This form must be filled out completely. ▪ The form is an Excel file that the EDE Entity will complete and submit to CMS.	▪ Submit via the DE/EDE Entity PME Site ▪ Prospective primary EDE Entities will receive an encrypted, pre-populated version of the form from CMS ▪ Prospective upstream EDE Entities will complete a blank version of the form that is available on CMS zONE	Both prospective primary and prospective upstream EDE Entities	Prospective primary EDE Entities: Submit with audit submission. Prospective upstream EDE Entities: Submit after the prospective primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for prospective upstream EDE Entities, but to be reasonably certain a prospective upstream EDE Entity will be approved by November 1, 2024, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1, 2024 or as soon as feasible to allow time to review prior to activating their Partner IDs.
EDE Business Requirements Audit Instructions and Report and Toolkits	▪ EDE Entities must submit the EDE Business Requirements Audit Instructions and Report Template and all applicable toolkits completed by its Auditor(s). ▪ See Section VI.B.ii, Business Requirements Audit Resources, Exhibit 5, for more information.	▪ The EDE Entity and its Auditor(s) must submit the different parts of the Auditor resources package via the DE/EDE Entity PME Site	Prospective primary EDE Entities, prospective phase change EDE Entities, and their Auditors	April 1-July 1 (3:00 AM ET)
Training	▪ EDE Entities (and their Auditors must complete the trainings as outlined in Section VIII, Required Auditor and EDE Entity Training. ▪ The trainings are located on REGTAP (located at the following link: https://www.regtap.info/).	▪ The person taking the training must complete the course conclusion pages at the end of each module ▪ The EDE Entity and Auditor are NOT required to submit anything additional to CMS but must retain a copy of the training confirmation webpage to provide to CMS, if requested	Prospective primary EDE Entities, prospective phase change EDE Entities, prospective upstream EDE Entities, and Auditors	Trainings must be completed by prospective primary and phase change EDE Entities and Auditors prior to Audit Submission Prospective upstream EDE Entities must complete the training prior to approval to use the EDE pathway

Document	Description	Submission Requirements	Entity Responsible	Deadline
HUB Onboarding Form	▪ All EDE Entities must submit a new or updated Hub Onboarding Form to request EDE access. If an EDE Entity does not already have a Partner ID, the Hub will create a Partner ID for the EDE Entity upon receiving the Hub Onboarding Form.	▪ Follow instructions on the Hub Onboarding Form (located at the following link: https://zone.cms.gov/document/hub-onboarding-form) ▪ Send to HubSupport@sparksoftcorp.com	Prospective primary and prospective upstream EDE Entities	Prior to accessing the EDE APIs
Application Technical Assistance and Mini Audit Testing Credentials	▪ An EDE Entity must provide application technical assistance and mini audit testing credentials to CMS consistent with the process defined in Sections VI.C, Application Technical Assistance, and X.D, Audit Submission Compliance Review for Prospective Primary EDE Entities, below.	▪ Follow instructions on the EDE UI Eligibility Technical Assistance Credentials Form Template on CMS zONE	Prospective primary EDE Entities and prospective phase change EDE Entities	Submit with audit submission date

ii. Business Requirements Audit Resources

CMS has provided the following resources and templates for Auditors to review and/or complete as part of each business requirements audit. The resources will be available on CMS zONE.[73]

For Year 7 of EDE, CMS will provide an updated Auditor resources package that will contain the following:

- *EDE Business Requirements Audit Instructions and Report Template:* The template will provide an outline and instructions for the contents of the business requirements audit report. Auditors will use this template to document a prospective EDE Entity's compliance with all business requirements, including those that the Auditor has reviewed using CMS-provided toolkits. Auditors must carefully review the instructions in the EDE Business Requirements Audit Instructions and Report Template.
- *Toolkits*: The Auditor resources package will contain multiple toolkits, each of which will correspond with one or more of the business requirements set forth in Exhibit 2. Each toolkit will provide testing scenarios that the Auditor will use to verify the prospective EDE Entity's compliance with the corresponding requirement(s). Each toolkit will contain a template that lists each scenario or requirement and provides a space for the Auditor to indicate the prospective EDE Entity's compliance. The prospective EDE Entity must submit the completed templates to CMS as part of the business requirements audit package. CMS will provide toolkits for the Eligibility Results Testing, API Functional Integration Testing, Application UI, and Consumer Communications requirements.
    - **Note:** CMS will identify baseline versions of each toolkit in early 2024. EDE Entities can use the baseline toolkit versions or a subsequently released version of the toolkit as the basis for the audit submission package for Year 7 of EDE. EDE Entities that begin their audit using the initial baseline toolkit versions are not required to switch to use subsequently released versions of the toolkits. However, CMS may designate specific changes made to subsequently released versions of the toolkits as CMS-initiated Change Requests. In order to receive final approval to use EDE, CMS will require EDE Entities to implement any CMS-initiated Change Requests with due dates that have elapsed before the EDE Entity's approval date consistent with the processes defined in Section XI.B, CMS-initiated Change Requests, prior to receiving CMS approval to use the EDE environment. CMS-initiated Change Requests may be issued throughout the year. Prospective EDE Entities should not begin their audits until CMS identifies the baseline toolkits and the Entity has completed its kickoff call and related pre-audit notification requirements (see Section X.A, Pre-Audit Notification to CMS). CMS recommends prospective EDE Entities not delay the start or completion of their audits in the interest of attempting to incorporate as many CMS-initiated Change Requests as possible in their initial audit submissions.

[73] The Business Audit documentation is available at the following link: https://zone.cms.gov/document/business-audit. Auditors can access CMS zONE through the EDE Auditor Community. EDE Entities must download the instructions for accessing the EDE Auditor Community, and provide the instructions to their Auditor(s). The instructions are labeled "accessing_the_ede_auditor_community.pdf." Auditors will need to be approved by CMS prior to gaining access to the EDE Auditor Community on CMS zONE. Auditor(s) should follow the instructions closely. Failure to do so may delay the EDE Auditor Community zONE approval process.

- **Note:** The Auditor must not modify or delete any language provided in any toolkit or template.
- **Note Regarding Phase-specific Requirements:** The Application UI and Eligibility Results Toolkits contain phase-specific requirements throughout the toolkits. Auditors and prospective EDE Entities must carefully review the **User Guide** tabs of these toolkits for information on how to identify the phase-specific requirements within the toolkits. For example, depending on the EDE Entity's selected end-state phase, the Auditor may need to complete multiple Eligibility Results Toolkits.

Exhibit 5 contains an overview of the documents available annually in the EDE Business Requirements Audit Instructions and Report Template and Toolkits zip file for Auditors and prospective EDE Entities to reference. CMS will label the zip file and documents with the appropriate plan year reference each year. For the year 7 audit submission window, CMS will label the files with PY2025.

Exhibit 5: EDE Business Requirements Audit and Report Template and Toolkits Zip File Documentation

Document	Description
EDE Business Requirements Audit Instructions and Report Template	The Business Requirements Audit Instructions and Report Template contains the instructions an EDE Entity and Auditor will need to complete the business audit. Additionally, the EDE Entity's Auditor will document their compliance findings related to the business audit requirements in Exhibit 2.
Application User Interface (UI) Toolkit	The Application UI Toolkit contains the application UI requirements. The toolkit also contains fields for the EDE Entity's Auditor to document their compliance findings related to the EDE Entity's implementation of the eligibility application. Note: Due to the phase-specific requirements in the Application UI Toolkit, EDE Entities and Auditors should carefully review the User Guide tab of the Application UI Toolkit. Note: If an EDE Entity has implemented a Spanish-language version of the Application UI, please review the Auditor User Guide of the Application UI Toolkit for instructions to document the compliance of the Spanish-language version of the Application UI Toolkit.
EDE Eligibility Results Toolkit (two phase-specific versions: Phase 2 and Phase 3)	The EDE Eligibility Results Toolkits contains phase-specific eligibility results test cases that the EDE Entity's Auditor will complete as required in the User Guide tabs. The toolkits also contain fields for the Auditor to document their compliance findings related to the EDE Entity's implementation of the eligibility application. Note: Due to the phase-specific versions of the EDE Eligibility Results Toolkit, EDE Entities and Auditors should carefully review the User Guide tabs of the EDE Eligibility Results Toolkit. Depending on the EDE Entity's phase, the EDE Entity may need to complete test cases from more than one of the phase-specific Eligibility Results Toolkits.
Communications Toolkit	The Communications Toolkit contains the Communications requirements and reference materials needed for an EDE Entity to implement CMS-required messaging. The toolkit also contains fields for the EDE Entity's Auditor to document their compliance findings related to the EDE Entity's implementation of the Communications requirements. Note: If an EDE Entity has implemented a Spanish-language version of the Communications requirements, please review the Auditor User Guide of the Communications Toolkit for instructions to document the compliance of the Spanish-language version of the Communications requirements.
API Functional Integration Toolkit	The API Functional Integration Toolkit contains test cases that the EDE Entity's Auditor will conduct to test various API-, application-, and communications-related functionality. The toolkit also contains fields for the EDE Entity's Auditor to document their compliance findings related to the expected results for each test case.

Document	Description
Other Supplemental Materials	The EDE Business Audit Instructions and Report Template and Toolkit file also contains reference materials needed to implement the requirements detailed in the toolkits, including test data sets, communications reference materials, application reference materials, and Spanish-language reference materials.

C. Application Technical Assistance

i. Mandatory UI Eligibility Technical Assistance (TA) Review Processes

The UI Eligibility TA Review process described in this section is a separate process from the optional UI Flexibility Consults (described below) and the audit review and mini audit process discussed in Section X.D, Audit Submission Compliance Review. During the UI Eligibility Technical Assistance Review, CMS will access the prospective primary or prospective phase change EDE Entity's test (pre-production) environment to conduct testing and evaluate API efficiency. The purpose of the required UI Eligibility TA Review process is to help mitigate the risk that CMS identifies compliance issues during the CMS-conducted mini audit (discussed in Section X.D, Audit Submission Compliance Review).

All prospective primary and prospective phase change EDE Entities must provide testing environment credentials using the Eligibility Technical Assistance Testing Team Credentials Form posted on CMS zONE.[74] Prospective primary and phase change EDE Entities will complete the Eligibility Technical Assistance Testing Team Credentials Form to submit credentials for the Eligibility TA Review as well as the Compliance Testing Team Credentials Form for the mini eligibility application audit, as detailed in Section X.D, Audit Submission Compliance Review. Prospective primary and phase change EDE Entities must submit two separate sets of credentials to access their Consumer-facing test environments (if applicable), and two separate sets of credentials (i.e., Eligibility Technical Assistance Testing Team Credentials Form and Compliance Testing Team Credentials Form) to access their Agent and Broker-facing test environments (if applicable). For example, EDE Entities pursuing approval to use both pathways will submit four sets of credentials, but Entities pursuing approval to use only the Consumer pathway or only the Agent and Broker pathway will submit two sets of credentials. The prospective primary or phase change EDE Entity must ensure that the testing credentials are valid and that all APIs and components of its EDE implementation in its testing environment are accessible for the duration of the UI Eligibility Technical Assistance Review. CMS will conduct the UI Eligibility TA Review when an EDE Entity's UI is complete and ready for review. Prospective EDE Entities do not need to wait until the business audit has been submitted to provide CMS with test environment credentials for CMS to begin conducting the UI Eligibility TA Review process. CMS recommends submitting a UI Flexibility Consult prior to the UI Eligibility TA Review.

Similar to the audit compliance review processes defined in Section X.D, Audit Submission Compliance Review, the application TA process will entail multiple rounds of feedback while a prospective primary or phase change EDE Entity attempts to resolve the risks identified by CMS during the UI Eligibility TA Review. This TA process is required, and a prospective primary or

[74] "Eligibility Technical Assistance Testing Team Credentials Form" located at https://zone.cms.gov/document/eligibility-enrollment-information.

phase change EDE Entity may be unable to progress in the audit queue until they have resolved critical risks identified during the TA process.

ii. Optional UI Flexibility Consults

Prior to conducting and submitting an audit, CMS strongly encourages a prospective primary or phase change EDE Entity to request feedback from CMS on its planned application UI build. CMS refers to this as a UI Flexibility Consult. UI Flexibility Consults consist of questions, screenshots, and/or narrative descriptions of a proposed application UI build. EDE Entities should submit UI Flexibility Consults through the DE/EDE Entity PME Site.[75] The purpose of this process is to answer clarifying questions about application requirements and discuss application UI innovation with subject matter experts at CMS. Requests should contain specific questions related to UI development, such as policy guidance, application requirements and flexibilities, technical design, and high-level application requirements and flow. Prospective primary and phase change EDE Entities should use the form provided by CMS on CMS zONE to request a UI Flexibility Consult.[76]

A prospective primary or phase change EDE Entity may submit UI Flexibility Consult requests up until the completion of the business requirements audit; upon submission of the audit, the prospective primary or phase change EDE Entity's application must be finalized. Upon submission of the audit, any Entity-initiated changes—that CMS has not identified and reviewed as part of the audit submission review activities—must follow the process described in Section XI.A, EDE Entity-initiated Change Requests.

CMS may release updated application guidance based on feedback received. While CMS may provide UI Flexibility Consult feedback to prospective primary and phase change EDE Entities on the application and UI, the Entity's Auditor should still include a compliance determination with respect to all requirements consistent with these Guidelines and other guidance.

iii. Best Practices Prior to the Audit

Prospective primary and phase change EDE Entities must complete development of their EDE environments and any related systems prior to initiating their audits, which includes integrating with all required APIs. Based on experience with previous audit submissions, it is strongly recommended that prospective primary and phase change EDE Entities complete development of their environments prior to the start of the audit submission window.

CMS strongly encourages prospective primary and phase change EDE Entities to test their environments using the supplemental EDE Partner Test Case Suite[77] in addition to all applicable required test cases contained in the toolkits. Please note, while the Eligibility Results Toolkit and API Functional Integration Toolkit include test cases to validate whether prospective primary and phase change EDE Entity environments can successfully complete certain scenarios, these should not be the only test cases that prospective primary and phase change EDE Entities rely on

[75] Please refer to Section IX, DE/EDE Entity Program Management Environment (PME) Site for Document Submission.

[76] "Requesting a UI Flexibility Consult" located at https://zone.cms.gov/document/eligibility-enrollment-information.

[77] Please refer to the EDE Partner Test Cases and EDE Partner Test Cases User Guide, available on CMS zONE at the following link: https://zone.cms.gov/document/eligibility-enrollment-information.

to confirm their EDE environments work appropriately in all scenarios. If a prospective primary or phase change EDE Entity utilizes, and can successfully complete, the supplemental EDE Partner Test Cases, the prospective primary or phase change EDE Entity will increase the likelihood that it will be approved without delay due to eligibility application or API risks. In addition, it is strongly recommended that prospective primary and phase change EDE Entities not begin the business requirements portion of their third-party audits (i.e., that use the Eligibility Results Toolkits, API Functional Integration Toolkit, Communications Toolkit, or the Business Audit Instructions and Report Template) until CMS releases the new baseline versions of each toolkit and template in early 2024. As detailed in Section VI.B.ii, Business Requirements Audit Resources, if a prospective primary or phase change EDE Entity begins the business requirements portion of their third-party audit prior to CMS releasing the baseline toolkits, the prospective primary or phase change EDE Entity and its Auditor may need to re-test some or all of the test cases using the baseline toolkit. CMS will reject audits as incomplete if they have not used the baseline toolkits, X.C.i, Submitting a Complete Business Requirements Audit.

VII. Privacy and Security Audit Requirements and Scope

An Auditor must complete the Security and Privacy Controls Assessment Test Plan (SAP), which must be submitted to CMS for review at least thirty (30) days prior to initiating the Security and Privacy Controls Assessment (SCA) portion of the audit. The Auditor will complete a privacy and security audit utilizing the NEE SSP Template[78] to ensure that the prospective EDE Entity complies with applicable requirements as defined in HHS regulations and these Guidelines. The Auditor must use NIST SP 800-53A[79] which describes the appropriate assessment procedure (examine, interview, and test) for each control to evaluate that the control is effectively implemented and operating as intended. A prospective EDE Entity must submit the resulting privacy and security audit package to CMS consistent with VII.A.i, Required Privacy and Security Audit Documentation, below.

CMS will allow EDE Entities to leverage prior audits that assessed some or all controls to satisfy some or all of the privacy and security audit requirements. To leverage a prior audit, the prior audit must have been conducted within one year of the date the EDE Entity submits its current audit documentation to CMS. Exhibit 6 describes the review areas and review standards for the privacy and security requirements. The findings of the Auditor reviews are to be documented in the Security Privacy Assessment Report (SAR).

[78] The current NEE SSP Template is based on NIST SP 800-53 Rev. 4.

[79] The current NEE SSP Template is based on NIST SP 800-53 Rev. 4 so Auditors should refer to the NIST SP 800-53 A for Rev. 4.

Exhibit 6: Privacy and Security Requirements

Review Category	Audit Standards
Privacy and Security Control Implementation	▪ *Requirement:* An EDE Entity must implement security and privacy controls, a fully completed NEE SSP, as well as other privacy and security standards, for protecting the confidentiality, integrity, and availability of the information collected, used, disclosed, and/or retained by the EDE Entity as defined in the ISA, EDE Business Agreement, and applicable laws and regulations prior to conducting the privacy and security audit. ▪ *Review Standard*: The Auditor must conduct a SCA and produce a SAR using the NIST SP 800-53A methodology to certify that the EDE Entity has implemented processes sufficient to meet the privacy and security requirements set forth in the ISA and EDE Business Agreement and in applicable laws and regulations. ▪ If the Auditor determines that the EDE Entity does not meet one or more privacy and security requirements, the EDE Entity must create a plan of action and milestones (POA&M) to resolve the deficiency. The POA&M should include a corrective action plan that explains how the EDE Entity will come into compliance with each requirement and will state the estimated completion date for each identified milestone. Monthly reviews and updates are required to be submitted to CMS until all significant findings are resolved based on findings from SCAs, security impact analyses, and continuous monitoring activities outlined in the ISCM Strategy Guide. Auditors must verify that the EDE Entity's EDE environment complies with the privacy and security standards, and that the environment and related website(s) is consistent with third-party data collection tools and standards defined by CMS in guidance; CMS regulations; and subsequent technical, and training documents. Additional information can be found in the EDE Privacy/Security Standards training module.
Concurrent Session Testing (NEE SSP AC-2: Account Management & AC-10 Concurrent Session Control)	▪ *Requirement*: The information system for all primary EDE Entities, hybrid issuer upstream EDE Entities implementing single sign-on, and hybrid non-issuer upstream EDE Entities must prohibit agent/broker use of concurrent sessions by FFE user ID. ▪ *Review Standard*: The Auditor must validate and document in the SAR the following: – Concurrent Session Control: The EDE Entity is able to effectively prohibit agent/broker use of concurrent sessions by FFE User ID. – Account Management: The EDE Entity is able to effectively block the creation of an additional account where the account creation is attempted using the same FFE User ID. EDE Entities that are unable to effectively block the creation of an additional account where the account creation is attempted using the same FFE User ID must have an end-to-end traceability mechanism that allows for more than one account to be created using the same FFE User ID while providing the ability to trace multiple accounts back to a single user.
Remote Access Testing (NEE SSP AC-17: Remote Access)	▪ *Requirement:* EDE Entity and its assignees or contractors—including, employees, developers, agents, and representatives—cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to EDE Entity's systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through VPN. ▪ *Review Standard:* The Auditor must validate and document in the SAR the existence of automated mechanisms to monitor and control remote access methods. The Auditor must verify that automated mechanisms block IP addresses located outside of the United States of America or its territories, embassies, or military installations attempting to access the EDE environment.

The primary EDE Entity's privacy and security audit boundaries should include any system(s) supporting the Entity's QHP shopping experience if a distinct system or systems hosting QHP shopping exist and the system(s) will exchange and/or store data.[80] If the primary EDE Entity's

[80] See, *supra*, notes 29-31.

EDE environment is sharing data with another environment it controls that is not within its EDE privacy and security audit boundary or with an upstream EDE Entity, the primary EDE Entity must document this arrangement in its ISA Appendix B as a data exchange between the primary EDE Entity and the upstream EDE Entity or between its own EDE and non-EDE environments. If the primary EDE Entity will not share EDE-specific eligibility data received via the Exchange APIs (e.g., SVI or DMI information) with the system(s) hosting the Entity's QHP shopping experience (whether the QHP shopping experience is hosted by a primary EDE Entity or an upstream EDE Entity), then the primary EDE Entity must work with its Auditor to fully document the approach the Entity is taking to meet applicable EDE requirements without sharing this data between systems.[81]

A. Audit Documentation

i. Required Privacy and Security Audit Documentation

Exhibit 7 contains the required information that prospective primary; hybrid issuer upstream, if applicable; and hybrid non-issuer upstream EDE Entities must maintain and submit, as applicable, to CMS as part of their privacy and security audits to be approved to participate in EDE.

Exhibit 7: Privacy and Security Audit Information Requirements

Document	Description	Submission Requirements	Entity Responsible	Deadline
Interconnection Security Agreement (ISA)	▪ A prospective primary EDE Entity must submit the ISA to use the EDE pathway. ▪ CMS will countersign the ISA after CMS has reviewed and approved the EDE Entity's business requirements audit and privacy and security audit.	▪ A prospective primary EDE Entity must submit the ISA via the DE/EDE Entity PME Site. ▪ The ISA contains Appendices that must be completed in full for an EDE Entity to be considered for approval. ▪ Appendix B of the ISA must detail: (1) all arrangements with upstream EDE Entities and any related data connections or exchanges, (2) any arrange-ments involving web-brokers, and (3) any arrangements with downstream agents and brokers that involve limited data collections, as described in Section IV.B., Downstream Third-party Agent and Broker Arrangements. ▪ Appendix B of the ISA must be updated and resubmitted, with changes noted in the change log, as a primary EDE Entity adds or changes any of the arrangements noted above consistent with the requirements in the ISA.	▪ Prospective primary EDE Entities	▪ Submit with the audit submission

[81] For example, audit requirements that may be affected by this implementation may include the following: post-enrollment communications requirements and the DMI and SVI action items requirements in the Communications Toolkit.

Document	Description	Submission Requirements	Entity Responsible	Deadline
Security Privacy Controls Assessment Test Plan (SAP)	▪ This report is to be completed by the Auditor and submitted to CMS prior to initiating the audit. ▪ The SAP describes the Auditor's scope and methodology of the assessment. The SAP includes an attestation of the Auditor's independence.	▪ A prospective EDE Entity and its Auditor must submit the SAP completed by its Auditor via the DE/EDE Entity PME Site.	▪ Prospective primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities	▪ At least thirty (30) days before commencing the privacy and security audit; during the planning phase
Security Privacy Assessment Report (SAR)	▪ This report details the Auditor's assessment findings of the prospective EDE Entity's security and privacy controls implementation.	▪ A prospective EDE Entity and its Auditor must submit the SAR completed by its Auditor via the DE/EDE Entity PME Site.	▪ Prospective primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities	▪ April 1 – July 1 (3:00 AM ET)
Plan of Action & Milestones (POA&M)	▪ A prospective EDE Entity must submit a POA&M if its Auditor identifies any privacy and security compliance issues in the SAR. ▪ The POA&M details a corrective action plan and the estimated completion date for identified milestones.	▪ A prospective EDE Entity and its Auditor must submit the POA&M in conjunction with the SAR via the DE/EDE Entity PME Site. ▪ POA&Ms with outstanding findings must be submitted monthly to CMS until all the findings from security controls assessments, security impact analyses, and continuous monitoring activities described in the NEE SSP controls CA-5 and CA-7 are resolved. Prospective EDE Entities can schedule their own time for monthly submissions of the POA&M, but must submit an update monthly to CMS until all significant or major findings are resolved. Thereafter, quarterly POA&M submissions are required as part of the ISCM activities.	▪ Prospective primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities	▪ Initial: April 1– July 1 (3:00 AM ET) ▪ Monthly submissions, as necessary, if outstanding findings. ▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit quarterly POA&Ms by the last business day of March, June (coincides with annual submission), August (due to Open Enrollment dependencies, all high and critical findings must be remediated by September 30), and December.

Document	Description	Submission Requirements	Entity Responsible	Deadline
Risk Acceptance Form	▪ The Risk Acceptance Form records the weaknesses that require an official risk acceptance from the organization's Authorizing Official. ▪ Before deciding to accept the risks, the relevant NEE's authorities should rigorously explore ways to mitigate the risks.	▪ Once the risk has been identified and deemed acceptable by the NEE's authorized official, the NEE must complete the entire Risk Acceptance Form and submit the completed form to CMS. The NEE will continue to track all accepted risks in the NEE's official POA&M.	▪ Prospective primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities	▪ The Risk Acceptance Form should be submitted with the POA&M during the regular POA&M submission schedule.
Privacy Impact Assessment (PIA)	▪ The PIA will detail the prospective EDE Entity's evaluation of its controls for protecting PII.	▪ A prospective EDE Entity is not required to submit the PIA to CMS. However, per the ISA, CMS may request and review an EDE Entity's PIA at any time, including for audit purposes.	▪ Prospective primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities	▪ Before commencing the privacy and security audit as part of the NEE SSP
Non-Exchange Entity System Security and Privacy Plan (NEE SSP)	▪ The NEE SSP will include detailed information about the prospective EDE Entity's implementation of required security and privacy controls. ▪ The SSP is required to be completed by the prospective EDE Entity and presented to the Auditor for evaluation of control implementation.	▪ A prospective EDE Entity is not required to submit the SSP to CMS. However, per the ISA, CMS may request and review an EDE Entity's SSP at any time, including for audit purposes.	▪ Prospective primary and hybrid non-issuer upstream EDE Entities	▪ Before commencing the privacy and security audit
Incident Response Plan and Incident/ Breach Notification Plan	▪ A prospective EDE Entity is required to implement breach and incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures. ▪ A prospective EDE Entity must incorporate these procedures into its own written policies and procedures.[82]	▪ A prospective EDE Entity is not required to submit the Incident Response Plan and Incident/Breach Notification Plan to CMS. A prospective EDE Entity must have procedures in place to meet CMS security and privacy incident reporting requirements. CMS may request and review an EDE Entity's Incident Response Plan and Incident/Breach Notification Plan at any time, including for audit purposes.	▪ Prospective primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities	▪ Before commencing the privacy and security audit as part of the NEE SSP

[82] https://www.cms.gov/files/document/rmh-chapter-08-incident-response.pdf.

Annual Penetration Testing	▪ The penetration test must include the EDE environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10. ▪ Before conducting the penetration testing, the EDE Entity must execute a Rules of Engagement with their Auditor's penetration testing team. ▪ The EDE Entity must also notify their CMS designated technical counterparts on their annual penetration testing schedule and must provide the following information to CMS, a minimum of five (5) business days using the CMS-provided form[83], prior to initiation of the penetration testing: – Period of testing performance (specific times for all penetration testing should be contained in individual test plans); – Target environment resources to be tested (IP addresses, Hostname, URL); and – Any restricted hosts, systems, or subnets that are not to be tested. ▪ During the penetration testing, the Auditor's testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment. ▪ The penetration testing shall be conducted in the lower environment	▪ A prospective EDE Entity and its Auditor must submit the Penetration Test results with the SAR via the DE/EDE Entity PME Site.	▪ Prospective primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities	▪ Initial: April 1–July 1 (3:00 AM ET) ▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities perform penetration testing and submit results to CMS annually, prior to last business day in June.

Document	Description	Submission Requirements	Entity Responsible	Deadline
	that mirrors the production environment.			
Vulnerability Scan	▪ A prospective EDE Entity is required to conduct monthly Vulnerability Scans.	▪ A prospective EDE Entity and its Auditor must submit the last three months of their Vulnerability Scan Reports, in conjunction with POA&M and SAR via the DE/EDE Entity PME Site. ▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&M. ▪ Similar findings can be consolidated.	▪ Prospective primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities.	▪ Initial: April 1–July 1 (3:00 AM ET) ▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit Vulnerability Scans with their quarterly POA&M submissions.

ii. Privacy and Security Audit Resources

CMS will provide the following resources and templates for Auditors to review and/or complete as part of each privacy and security audit. The resources will be available on CMS zONE.[84]

CMS will provide an Auditor resources package that will contain the following[85]:

- **Framework for the Independent Assessment of Security and Privacy Controls (Framework):** The Framework will provide an overview of the independent security and privacy assessment requirements. The Auditor should review the Framework prior to conducting the privacy and security audit.
- **Non-Exchange Entity System Security and Privacy Plan (SSP) Template and Final SSP:** The prospective EDE Entity will use the NEE SSP Template to create a final NEE SSP, which will include detailed information about the prospective EDE Entity's implementation of security and privacy controls. The Auditor will review the NEE SSP Template and final NEE SSP to make its assessment of the prospective EDE Entity's compliance with the required privacy and security controls.
- **Security and Privacy Controls Assessment Test Plan (SAP) Template:** The SAP will contain a high-level description of the critical items that the Auditor must test. The Auditor and the prospective EDE Entity must supply this document and submit it to CMS for review prior to conducting the privacy and security audit.
- **Security & Privacy Assessment Report (SAR) Template:** The Auditor is required to use this template to document the audit findings whether the prospective EDE Entity has implemented the required privacy and security controls correctly.

[83] The Penetration Testing Notification Form is available at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

[84] The Privacy and Security Audit documentation is available at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

[85] The resource templates are available at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

- **Plan of Action and Milestones (POA&M) Template:** The prospective EDE Entity will be required to use this template to create a POA&M. The POA&M entries are created within thirty (30) days of the results for every internal/external audit/review or test (e.g., security controls assessment, penetration test) to document the EDE Entity's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security and privacy controls and to reduce or eliminate known vulnerabilities. The POA&Ms should be submitted to CMS by prospective EDE Entities monthly until all significant vulnerabilities are remediated. CMS requires approved primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities to submit quarterly POA&Ms and Vulnerability Scans by the last business day of March, June (coincides with annual submission), August (due to Open Enrollment dependencies, all high and critical findings must be remediated by September 30), and December.
- **Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide:** The ISCM Strategy Guide provides the minimum requirements for an EDE Entity to implement an ISCM program for its systems and to maintain ongoing CMS authorization and approval to participate in EDE. ISCM provides a mechanism for an EDE Entity to identify and respond to new vulnerabilities, evolving threats, and constantly changing enterprise architecture and operational environments, such as changes in the hardware or software, as well as data creation, collection, disclosure, access, maintenance, storage, and use. Ongoing assessment and authorization provides CMS a method of detecting changes to the security and privacy posture of an EDE Entity's IT system that are essential to making well-informed, risk-based decisions. Approved primary, hybrid issuer upstream, and hybrid non-issuer upstream EDE Entities are required to submit ISCM packages by the last business day of June.
- **Risk Acceptance Form:** The Risk Acceptance Form records the weaknesses that require an official risk acceptance from the EDE Entity's Authorizing Official. The relevant EDE Entity's authorities should rigorously explore ways to mitigate the risks before deciding to accept them. Once all options are exhausted, accepting some manageable level of risk might be the unavoidable outcome. It is imperative to clearly describe the overview of the risk along with its source in the Risk Acceptance Form. The Risk Acceptance Form identifies the responsible entities and stakeholders of this process and the necessary mitigation procedures essential to the risk acceptance decision. It provides context about the risk acceptance process and specifies the required activities to complete form. The Risk Acceptance Form should be submitted with the POA&M during the regular POA&M submission schedule.

VIII. Required Auditor and EDE Entity Training

Representative(s) from all prospective and existing EDE Entities (including prospective phase change and upstream EDE Entities) are required to take CMS-mandated trainings, as summarized in Exhibit 8.

The Auditor(s) selected by the prospective EDE Entity (including applicable hybrid issuer, hybrid non-issuer upstream, and a prospective phase change EDE Entity) are also required to take CMS-mandated training, as summarized in Exhibit 8.

All Auditor representatives responsible for conducting the business requirements audit and/or the privacy and security audit must take the required trainings relevant to the audit(s) they are

conducting. The same individual from each respective EDE Entity and Auditor does not need to complete all trainings; in this situation, CMS expects that an individual would take the training most suited to the individual's role in conducting the audit or implementing the EDE environment. However, each module must be completed by at least one representative from the Auditor and EDE Entity.

Exhibit 8: Auditor and EDE Entity Training Requirements

Business Requirements Auditor Training Requirements	Privacy and Security Auditor Training Requirements	Prospective EDE Entity Training Requirements	Existing EDE Entity Training Requirements
• An Auditor who will be completing the business requirements audit must complete the following training modules before initiating that audit: - Regulator and Compliance Standards, - Application User Interface, - ORR and CMS Reporting Requirements, and - EDE Non-Eligibility API Guidance.	• An Auditor who will be completing the privacy and security audit, including Auditors for prospective upstream EDE Entities, must complete the following training modules before initiating the audit: - Regulatory and Compliance Standards and - Security and Privacy Standards.	• **Primary EDE Entities**: Representative(s) from the prospective primary EDE Entity must take all training modules. The same representative does not need to take all trainings, if only a few are relevant to their job area; however, each module must be completed by at least one representative from the EDE Entity. • **Upstream EDE Entities**: CMS requires representatives from upstream EDE Entities to take the following three training modules. The same representative does not need to take all trainings, if only a few are relevant to their job area; however, each module must be completed by at least one representative from the EDE Entity: - Regulatory and Compliance Standards, - ORR and CMS Reporting Requirements, and - Security and Privacy Standards.	• **Existing Primary and Upstream EDE Entities**: Representative(s) from the existing primary and upstream EDE Entities must retake the following three updated training modules: - Regulatory and Compliance Standards, - ORR and CMS Reporting Requirements, and - Security and Privacy Standards.

The trainings are self-paced computer-based trainings (CBTs) and provide information about compliance, EDE technical requirements, privacy and security, and reporting requirements. CMS will release further information regarding the trainings via REGTAP and anticipates the trainings for Year 7 of EDE will become available beginning in early 2024. All training modules will be posted on REGTAP as they become available.[86]

[86] REGTAP can be accessed at the following link: https://www.regtap.info/.

Trainings from the PY 2024 OEP approval process (Year 6 of EDE) are still available on REGTAP; however, CMS will release updates to these modules in early 2024 for Auditors and EDE Entities to take the revised modules (i.e., trainings for Year 7 of EDE). EDE Entities and their Auditors may take the existing trainings from Year 6 of EDE that currently exist on REGTAP prior to starting the audit instead of waiting for the updated trainings. EDE Entities and their Auditors who opt to do so must still take the updated trainings for Year 7 prior to submitting the audit. EDE Entities and their Auditors will be accountable for any updates in the updated trainings if they take this approach (i.e., they take the trainings from Year 6 of EDE prior to taking the trainings for Year 7 of EDE, they must still take the updated trainings for Year 7 prior to submitting the audit(s)).

IX. DE/EDE Entity Program Management Environment (PME) Site for Document Submission

CMS requires EDE Entities to submit documents to CMS via its DE/EDE Entity PME site. After the Entity informs CMS that it has entered into an agreement with its Auditor(s), CMS will provide the Entity with instructions to establish a DE/EDE Entity PME site that the Entity will use to access and upload documents to the portal.[87] CMS will also provide written instructions for using the DE/EDE Entity PME site via email at that time. CMS will not require EDE Entities to encrypt documents containing proprietary information before uploading them to the site.

X. Approval Process and Audit Submission Window

The EDE approval process consists of the following phases, as described further in this section: pre-audit notification to CMS; audit submission; audit submission completeness review; audit submission compliance review; final approval process; and post-EDE-approval oversight processes.

A. Pre-Audit Notification to CMS

Once an Entity has contracted with an Auditor(s) to complete the two parts of the ORR, the Entity's privacy and security Auditor must complete the NEE SSP and the SAP. The NEE SSP must be submitted to CMS for review prior to conducting the privacy and security audit. The SAP must be submitted to CMS for review thirty (30) days prior to conducting the privacy and security audit. The Entity must also submit a copy of the signed agreement or contract between the Auditor(s) and Entity as part of the notice of intent, as detailed in Section VI.B.i, Required Business Requirements Audit Documentation. The contract must describe the Auditor's entire scope of work and include provisions consistent with 45 C.F.R. § 155.221(g). The Entity may redact information (e.g., pricing and proprietary information) that is not necessary for CMS review. The Entity must notify DE Support (directenrollment@cms.hhs.gov) before its Auditor begins its audits (at least two weeks prior). CMS will schedule a kickoff call with the Entity and the Auditor(s) before the audits are initiated to answer questions, ensure expectations are clear, and ensure the Auditor(s) and Entity are using the correct audit documents. CMS may schedule additional calls as necessary.

[87] Instructions on how to request a DE/EDE Entity PME Site are available on CMS zONE at the following link: https://zone.cms.gov/document/business-audit.

B. Audit Submission

Prospective primary EDE Entities interested in submitting an audit for an EDE environment in calendar year 2024 must submit business requirements and privacy and security audits and prospective phase change EDE Entities must submit the business requirement audit during the audit submission window from April 1, 2024 to 3:00 AM ET on July 1, 2024 (i.e., three hours after midnight on June 30, 2024). CMS will not accept audits received outside of this submission window for initial approval as a primary EDE Entity or for prospective phase change EDE Entities seeking to change application phases.[88] There is no guarantee that every prospective primary EDE Entity and prospective phase change EDE Entity that submits an audit in the submission window will receive approval to go live with EDE before the start of the PY 2025 OEP or even during calendar year 2024. If a prospective EDE Entity or prospective phase change EDE Entity submits an audit, and then resubmits its audit before receiving feedback from CMS, CMS will only consider the date of the latest submission for purposes of determining review priority. CMS will conduct an initial high-level review of each audit on a first come, first serve basis to evaluate the quality and completeness of the audit submitted.

If a prospective primary EDE Entity or prospective phase change EDE Entity intends to submit its audit during the April 1, 2024–July 1, 2024 (at 3:00 AM ET) submission window, it should submit its notice of intent, as detailed in Section VI.B.i, Required Business Requirements Audit Documentation, to directenrollment@cms.hhs.gov by March 1, 2024. CMS encourages prospective EDE Entities to submit as early as possible in the audit submission window (but no earlier than April 1, 2024); however, prospective EDE Entities should not submit incomplete audits, audits with material deficiencies, or audits that evaluated incomplete EDE environments or systems. Once an audit is deemed complete, CMS will review the audit submission for compliance as described in Section X.D, Audit Submission Compliance Review for Prospective Primary EDE Entities, and will work with the Entity to carry out the next steps in the approval process[89] and will provide additional feedback. If an Entity submits an incomplete audit, once the Entity resubmits its audit, CMS will prioritize that resubmitted audit at the end of the review queue. CMS does not guarantee any review or approval timelines.

CMS will conduct completeness reviews[90] on all prospective primary EDE Entity and prospective phase change EDE Entity audits submitted during the audit submission window. CMS does not guarantee that an Entity will have an opportunity to correct an incomplete audit submission within the audit submission window. **Prospective primary EDE Entities and prospective phase change EDE Entities that submit late in the audit submission window may not have an opportunity to remediate completeness findings.** If CMS deems an audit incomplete or if the EDE Entity submits the remedial documentation after the audit submission window has closed (July 1, 2024 at 3:00 AM ET), the next opportunity the prospective primary

[88] CMS will accept prospective hybrid non-issuer upstream EDE Entity privacy and security and business requirements audits on a rolling basis.

[89] Prospective EDE Entities may utilize the Program Participation Checklist, available at the following link: https://zone.cms.gov/document/general-ede-guidance-and-information, as a resource summarizing the EDE approval process. CMS will update and deliver the Program Participation Checklist to prospective EDE Entities after CMS has determined its audit submission is complete and throughout the approval process.

[90] Please refer to Section X.C, Audit Submission Completeness Review.

EDE Entity and prospective phase change EDE Entity would have to attempt to submit an audit would be during the next audit submission window.[91]

As previously stated, the EDE approval process typically takes many months, and may take a year or more depending on the selected end-state application phase, the quality of the build of the EDE environment, the quality of the audit and documentation submitted to CMS, and the quality and timeliness of resubmissions. Based on CMS's experience with prior audits, prospective primary EDE Entities and prospective phase change EDE Entities that submit complete audits later in the audit window (i.e., mid-to-late May through June), depending on the quality of the submission and phase, have a lower probability of going live before the subsequent OEP.

CMS expects to issue updated trainings (required for both Auditors and representatives of EDE Entities), agreements, and baseline toolkits for the April 1, 2024–July 1, 2024 audit submission window in early 2024. CMS expects to primarily use the same content as the materials released in 2023, with updates to reflect any new applicable guidelines or standards. Accordingly, prospective primary EDE Entities and prospective phase change EDE Entities can begin developing their EDE environments based on the existing toolkits and privacy and security documentation that are located on CMS zONE.[92] CMS will continue to update these toolkits throughout the audit submission window and after it closes. EDE Entities must use at least the baseline version of the toolkits for the audit submission (as designated by CMS prior to the audit window), but can choose to use a later, updated version of a toolkit, if available. Important note: EDE Entities are only required to build to the baseline version of each toolkit for the audit submission. All subsequent toolkit updates that the EDE Entity must implement will be released as CMS-initiated Change Requests.[93]

C. Audit Submission Completeness Review

i. Submitting a Complete Business Requirements Audit

CMS will review each business requirements audit submission for completeness on a first come, first serve basis. CMS will not accept incomplete audits. A complete business requirements audit submission meets the criteria described in Exhibit 9, at a minimum. CMS strongly encourages entities to review these requirements thoroughly to avoid having their audits rejected during the audit submission window.

[91] Similar to the audit submission windows in prior years, CMS expects to open an audit submission window in the first half of each calendar year.

[92] The Business Requirements Audit documentation is available at the following link: https://zone.cms.gov/document/business-audit. The Privacy and Security Audit documentation is located at the following link: https://zone.cms.gov/document/privacy-and-security-audit. Auditors can access CMS zONE through the EDE Auditor Community. EDE Entities must download the instructions for accessing the EDE Auditor Community and provide the instructions to their Auditor(s). The instructions are labeled "accessing_the_ede_auditor_community.pdf." Auditors will need to be approved by CMS prior to gaining access to the EDE Auditor Community on CMS zONE. Auditor(s) should follow the instructions closely. Failure to do so may delay the EDE Auditor Community zONE approval process. For more information on CMS zONE, please refer to Section XII.D, CMS zONE Communities (Guidance & Technical Resources).

[93] Please refer to Section XI.B, CMS-initiated Change Requests, for more information.

Exhibit 9: Business Requirements Audit Submission Requirements for a Complete Audit

Toolkit & Template	Minimum Requirements for a Complete Audit
All Toolkits	▪ Provide complete Auditor documentation (i.e., required columns indicated for Auditor results contain details regarding the Auditor's evaluation of the requirement, including compliance status, risks, and mitigation strategies (if applicable)). The Auditor's evaluation must contain no ambiguous language about potential unmitigated risks (e.g., stating that the Auditor has identified risks, or the prospective EDE Entity has mitigated the risks without a description of the risks or mitigation strategies). ▪ Complete screenshots that demonstrate all reviewed content without missing, obscured, or cut-off elements that are required to evaluate compliance with the requirements represented by the screenshot. ▪ All required rows, across all required tabs, of each toolkit are completed. Auditors should refer to the Auditor User Guide tab of each Toolkit to identify required tabs, columns, and rows. ▪ Risks identified during the course of the audit must be documented and explained, even if the EDE Entity has subsequently mitigated the risks (i.e., a history of initial risk identification and attempted mitigation through any and all subsequent reviews and mitigation attempts should be documented to enable CMS to understand the original and subsequent risks identified and how all risks were mitigated). ▪ The prospective EDE Entity may be required to continue engaging its Auditor after audit submission. – If the resubmission requires another audit of the requirement(s) in a template or a toolkit, the prospective EDE Entity is expected to engage its Auditor to confirm that the resubmitted requirement(s) is compliant. – The Auditor may be expected to engage in a phone call with CMS to discuss its compliance determinations and applicable entity mitigation strategies. • Prospective EDE Entities and their Auditors must submit all requested re-audited documentation, when requested by CMS (i.e., resubmit the entire Business Audit Package). This ensures that CMS has the full submission of updated documents in one complete package. ▪ Note: For any issues or risks identified during the completeness review that are attributable to CMS-confirmed Exchange defects, CMS will not hold prospective EDE Entities responsible for such defects; however, the prospective EDE Entity must confirm the defect exists with CMS help desk teams[94] and document that the issue exists in the applicable Toolkit or EDE Business Requirements Audit Instructions and Report Template. CMS may require the prospective EDE Entity demonstrate the required functionality once CMS has resolved the CMS-confirmed Exchange defect. For example, if a prospective EDE Entity is unable to complete an API Functional Integration Toolkit test case due to a CMS-confirmed Exchange defect, CMS may require the EDE Entity to submit the test case in full once CMS has resolved the defect.
Communications Toolkit	▪ Complete screenshots that demonstrate compliance when the applicable requirements require screenshots to be provided as evidence under the **Requirements** tab in the toolkit. ▪ EDE Entities of all phases must submit screenshots to support document upload requirements for all DMIs and SVIs. There are no phase-specific exceptions for the account management and document upload requirements. ▪ For any Communications Toolkit screenshots that involve multiple webpages or screens, EDE Entities must provide screenshots of all relevant webpages or screens (e.g., if the EDE Entity is providing a link to the consumer FAQs from the Communications Toolkit requirements, provide the screenshots of the link origin and destination).

[94] Please refer to Section XII.A, Help Desk, for more information on submitting tickets to the appropriate CMS help desk.

Toolkit & Template	Minimum Requirements for a Complete Audit
Application User Interface (UI) Toolkit	▪ The Application UI Toolkit must be reviewed in full and documented appropriately (see the "All Toolkits" minimum requirements above) for the applicable phase, which includes all UI elements included in that phase (e.g., an audit of a phase 3 application would include application questions that are also applicable to phase2, as well as application questions specific to phase 3 only). Note: The test cases in the Eligibility Results Toolkits do not cover all questions or requirements in the Application UI Toolkit. As a result, Auditors must develop a methodology to ensure each element of the Toolkit is evaluated. Prospective EDE Entities have the option to test a variety of functionalities in their UIs using additional, optional, EDE Partner Test Cases[95].
Eligibility Results Toolkit(s)	▪ Each phase has its own Eligibility Results Toolkit. Phase 2 EDE Entities must complete all phase 2 test cases. Phase 3 EDE Entities must complete all phase 3 test cases and some of the phase 2 test cases. Please refer to the User Guide tab in the Eligibility Results Toolkits for more specific test case instructions. Please note, depending upon an Entity's planned service areas, it may need to request modifications to test cases, as described in the User Guide tab in the Eligibility Results Toolkits. ▪ Screenshots of the entire application flow are provided for each test case from either the coverage year and coverage state questions (items #1 and #2 in the Application UI Toolkit) or the privacy notice disclaimer (item #3 in the Application UI Toolkit), whichever comes first in the Entity's environment, through the entire application including the eligibility results page. – Note: The screenshots described above are required for the toolkit associated with the entity's target application phase, but not for lower phase toolkits. For example, a prospective phase 3 EDE Entity would submit screenshots for the phase 3 Eligibility Results Toolkit test cases, but not phase 2 test cases. The EDN and JSON requirements described below apply to all required test cases across all required toolkits. For example, a prospective phase 3 EDE Entity would submit EDNs and raw JSONs from the Get App API Response for both phase 2 and phase 3 Eligibility Results Toolkit test cases. ▪ A screenshot depicting the eligibility results page with correct eligibility results and EDN are provided for each test case. The eligibility results must not differ between the eligibility results page and the EDN, and every element of the eligibility results should be correctly represented. ▪ A copy of the raw JSON from a Get App API Response for the application version depicted in the screenshots for each test case. ▪ CMS will review the eligibility results page and the EDN for the correct results for each applicant based on the Toolkits and consistent results between the eligibility results page and the EDN for the following elements: – Exchange OEP or SEP eligibility (QHP); – Advance payments of the premium tax credit (exact amount, if applicable); – CSRs; – Medicaid eligibility; – CHIP eligibility; – SVIs; and – Non-MAGI Medicaid Referral.

[95] Please refer to the EDE Partner Test Cases and EDE Partner Test Cases User Guide, available on CMS zONE at the following link: https://zone.cms.gov/document/eligibility-enrollment-information.

.

Toolkit & Template	Minimum Requirements for a Complete Audit
API Functional Integration Toolkit	▪ Correct results and successful completion of each test case is documented. – If an EDE Entity will pursue approval to use both the Consumer pathway and the Agent and Broker pathway, the submission must include documentation reflecting the expected results for each pathway. In other words, the EDE Entity must complete the full test case in both the Agent/Broker and Consumer pathways and submit the required documentation for each pathway. The EDE Entity may not use evidence from one pathway to satisfy the evidence for the other pathway (e.g., using screenshots or API calls from the Consumer pathway application to satisfy the requirement for the Agent/Broker pathway), if the EDE Entity must provide evidence for both pathways. ▪ Successful completion of the DMI and SVI test cases consistent with the Toolkit's instructions. ▪ Complete submission of all required evidence outlined in the "Required Evidence" column, Column H, on the "Test Cases" tab within the API Functional Integration Toolkit, including the complete header and body for each required API request and response. – JSONs and XML files submitted as required evidence for a Test Case must be raw and unmodified by the EDE Entity.
EDE Business Requirements Audit Instructions and Report Template	▪ Complete descriptions of each requirement; Auditors must not exclude required review criteria from their review and description of each requirement (e.g., the Requirement and Review Standard criteria for each business requirement).
DE Entity Documentation Package	▪ CMS requires that the prospective EDE Entity submit a complete DE Entity Documentation Package. While the prospective EDE Entity may need to re-submit documentation during EDE Agreement Renewal or prior to approval, CMS requires a complete DE Entity Documentation Package at audit submission to review the documentation for compliance.

An incomplete business requirements audit is an audit that does not meet the criteria described above. The Auditor must take the appropriate actions to complete the incomplete audit and the prospective EDE Entity must resubmit it, as applicable. Please review Section X.B, Audit Submission, for more information.

CMS will conduct an initial high-level review of all audit submissions in the order they are received and based on available resources. If a prospective EDE Entity submits an incomplete audit, CMS will communicate the missing elements to the Entity based on the initial high-level review and the audit will be removed from the audit review queue. The Entity may receive multiple rounds of feedback from CMS on its business requirements audit. It may take several weeks or more to resolve all missing elements prior to CMS accepting an Entity's audit submission. Consistent with the deadlines in Section X.B, Audit Submission, CMS will require that missing elements of incomplete audits be resubmitted by the EDE Entity or its Auditor, when an Auditor's re-evaluation is specifically required by CMS, and CMS will prioritize its review of these resubmitted audits based on the date the complete audit is submitted.

Audits should not include comments that describe the Auditor's process for verifying the requirement unless there is a specific issue or concern with respect to the requirement that warrants raising the concern to CMS.

ii. Submitting a Complete Privacy and Security Audit

CMS will review each privacy and security audit submission for completeness. CMS will not accept incomplete audits. A complete privacy and security audit submission meets the criteria described in Exhibit 10, at a minimum.

Exhibit 10: Privacy and Security Audit Submission Requirements for a Complete Audit

Document	Minimum Requirements for a Complete Audit
Security and Privacy Controls Assessment Test Plan (SAP)	▪ The SAP describes the Auditor's scope and methodology of the assessment. ▪ The SAP includes an attestation of the Auditor's independence. ▪ The SAP must be completed by the Auditor and submitted to CMS for review, prior to conducting the security and privacy controls assessment (SCA).
Non-Exchange Entity System Security and Privacy Plan (SSP)	▪ The NEE SSP will include detailed information about the prospective EDE Entity's implementation of required security and privacy controls. ▪ The implementation of security and privacy controls must be completely documented in the NEE SSP before the audit is initiated. ▪ The NEE SSP is a living document and should be reviewed and updated at least annually or whenever there is a change related to the security and privacy controls implementation.
Security Assessment Report (SAR)	▪ The SAR is not a living document; findings should not be added/removed from the SAR unless CMS' initial review of the final draft discovers deficiencies or inaccuracies that need to be addressed. ▪ The SAR should contain a summary of findings that includes ALL findings from the assessment to include documentation reviews, control testing, scanning, penetration testing, interview(s), etc. ▪ Explain if and how findings are consolidated. ▪ Ensure risk level determination is properly calculated, especially when weaknesses are identified as part of the Center for Internet Security (CIS) Top 18 and/or Open Web Application Security Project (OWASP) Top 10. ▪ Only one final SAR should be submitted to CMS. Once that SAR has been submitted and CMS has no additional comments or edits on the SAR, the prospective EDE Entity should not submit additional SARs.
Plan of Action and Milestones (POA&M)	▪ Ensure all open findings from the SAR have been incorporated into the POA&M. ▪ Explain if and how findings from the SAR were consolidated on the POA&M; include SAR reference numbers, if applicable. ▪ Ensure the weakness source references each source in detail to include type of audit/assessment and applicable date range. ▪ Ensure the weakness description is as detailed as possible to include location/server/etc., if applicable. ▪ Ensure scheduled completion dates, milestones with dates, and appropriate risk levels are included.

An audit that does not meet the criteria described above is an incomplete privacy and security audit. The Auditor must take the appropriate actions to complete the incomplete audit and the prospective EDE Entity must resubmit it, as applicable. The Entity may receive multiple rounds of feedback from CMS on its privacy and security audit. This process may take several weeks or more to resolve all missing elements prior to CMS accepting an Entity's audit submission. Consistent with the deadlines in Section X.B, Audit Submission, prospective EDE Entities with incomplete audits must resubmit complete audits and will not be reviewed further until the Entity submits an audit that CMS reviews and deems complete consistent with the completeness criteria in this section.

D. Audit Submission Compliance Review for Prospective Primary EDE Entities

After determining that all audits submitted by the prospective primary EDE Entity (e.g., the business requirements audit and privacy and security audit for a prospective primary EDE Entity) are complete, CMS will conduct a thorough compliance review of the entire audit package.[96] CMS will review the audit package with subject matter experts and generate compliance findings for the Entity to resolve. On both the privacy and security audit and the business requirements audit, the Entity should expect to receive multiple rounds of feedback from CMS. This process may take several months or more (e.g., potentially a year or more) to resolve all critical risks that the Entity must address prior to advancing in the audit queue. In order to progress through the audit queue, an Entity must thoroughly address the issues identified by CMS and provide sufficient documentation of the resolution of the risk(s). When CMS confirms that a prospective EDE Entity has resolved the critical risks identified during the compliance review of the business requirements audit package and any feedback from the CMS TA team, the EDE Entity will progress to the mini audit phase of the review process. During this next phase, CMS will conduct a mini audit of the Entity's application in its test environment prior to providing final approval of the Entity's EDE environment. The prospective EDE Entity must ensure that the testing credentials for the mini audit are valid and that all APIs and components of its EDE implementation in its testing environment are accessible for the duration of the mini audit. The mini audit is not intended to replicate an Auditor's review of a prospective EDE Entity's EDE environment; the mini audit focuses on reviewing a subset of eligibility scenarios for compliance.[97] The prospective EDE Entity must not make changes to its EDE environment after submitting its audit package, unless in response to a CMS request or feedback or in accordance with the EDE Entity-initiated CR protocol in Section XI.A, EDE Entity-initiated Change Requests.

CMS will review any compliance issues identified during the mini audit and provide written feedback to the prospective EDE Entity of changes that the prospective EDE Entity will be required to make prior to final approval. The prospective EDE Entity must notify CMS that it implemented the required changes. CMS will conduct subsequent validation testing and provide further feedback or approval.

Throughout the compliance review and mini audit process, CMS will regularly provide the prospective EDE Entity with a checklist that describes the prospective EDE Entity's progress through the EDE approval process. This checklist will allow a prospective EDE Entity to confirm the status of their audit review and any required documentation that must be submitted to CMS. CMS will establish status calls with a prospective EDE Entity that has submitted complete audits after CMS has provided compliance feedback to the prospective EDE Entity.

[96] This section discusses the process for a prospective primary EDE Entity; however, aspects of the compliance review process apply to other prospective EDE Entities that will submit audits to CMS. Please review Section X.G, Approval Process for Upstream EDE Entities with Audit Requirements, for a discussion of the compliance review process with respect to prospective upstream EDE Entities.

[97] CMS will not provide EDE Entities with the mini audit eligibility scenarios used to evaluate the prospective EDE Entity's EDE environment.

E. Final Approval Process

CMS will notify prospective EDE Entities on a rolling basis of approval to use the EDE pathway. Prospective EDE Entities may not be approved in the order in which their audits were submitted because the content and quality of the audit submissions vary substantially and that affects the amount of time it takes to review and approve a prospective EDE Entity's EDE environment. Once a prospective EDE Entity has resolved all critical business and privacy and security risks, the Entity will enter the "request to connect" phase. CMS will countersign a prospective EDE Entity's EDE Business Agreement and ISA after CMS reviews and approves the Entity's business requirements audit package and privacy and security audit package, and after CMS confirms that the Entity's EDE environment is functional. This will not occur until after the Entity enters the "request to connect" phase. After CMS countersigns the EDE Business Agreement and the ISA, CMS will engage with the Entity to determine a mutually agreed upon production go live date and time, and will coordinate with the Hub to enable EDE access to the production environment. Newly approved EDE Entities must work with CMS to complete the onboarding process in accordance with the scale and schedule set by CMS, in its sole discretion, until demonstrating that no significant errors exist that may pose a risk to Exchange systems. This process and final step to confirm full operational readiness may take several weeks or more depending on several factors, such as the EDE Entity's enrollment volume, whether the EDE Entity is onboarding upstream entities, and the overall enrollment Marketplace traffic occurring at the time of onboarding. Similarly, existing EDE Entities who are approved to implement a phase change (such as a EDE Entities upgrading from phase 2 to phase 3) may be directed by CMS to throttle their enrollment volume and/or onboard each new upstream entity separately to demonstrate that no significant errors exist as a result of the phase upgrade.

F. Post-EDE-Approval Oversight Processes

After CMS issues final approval, it will conduct periodic, post-go-live mini audits or other continuous monitoring activities as needed. If CMS identifies compliance issues after approval, pursuant to 45 C.F.R. § 155.221(e), CMS may immediately suspend the EDE Entity's EDE environment's connection to the EDE pathway until the Entity has addressed any identified compliance issues to CMS' satisfaction. If CMS identifies any compliance issues likely to affect a consumer's eligibility application or results, CMS may require the EDE Entity to take further action necessary to remediate any issues affecting consumers as a result of the compliance issues. CMS may, at its discretion, conduct mini audits or other continuous monitoring activities following any post-approval changes (see Section XI, Processes for Changes to an Audited or Approved EDE Environment) in an EDE Entity's EDE environment.

G. Approval Process for Upstream EDE Entities with Audit Requirements

The EDE audit approval process for upstream EDE Entities subject to audit requirements[98] depends on the exact functionality and systems implemented by the upstream EDE Entities. Regardless of the upstream EDE Entity's functionality, the upstream EDE Entity audit review and approval process is similar to the primary EDE Entity audit review and approval process (Section X.D, Audit Submission Compliance Review). CMS will review the audit package with

[98] Upstream EDE Entities with audit requirements include hybrid issuer upstream EDE Entities implementing SSO (Section IV.A.v Privacy and Security Audit Requirements for Hybrid Issuer Upstream EDE Entities Implementing Single Sign-On) and hybrid non-issuer upstream EDE Entities (Section IV.A.iv, Privacy and Security Audit Requirements for Hybrid Non-issuer Upstream EDE Entities).

subject matter experts and generate compliance findings for the Entity to resolve. For both the privacy and security audit and the business requirements audit (if applicable), the Entity should expect to receive multiple rounds of feedback from CMS. This process may take several months or more (e.g., potentially a year or more) to resolve all critical risks that the Entity must address prior to advancing in the audit queue. In order to progress through the audit queue, an Entity must thoroughly address the risks identified by CMS and provide sufficient documentation of the resolution of the risk(s). After resolving all risks, if CMS has already approved the upstream EDE Entity's primary EDE Entity, CMS will countersign the upstream EDE Entity's EDE Business Agreement and work with the Hub and the primary EDE Entity to activate the upstream EDE Entity's EDE connection.

XI. Processes for Changes to an Audited or Approved EDE Environment

A. EDE Entity-initiated Change Requests

i. EDE Entity-initiated Change Request Process

If an EDE Entity wishes to make changes to its audited or approved EDE environment or functionality that are not in response to an Auditor's documented findings, CMS feedback or requests, or compliance findings, the EDE Entity must follow the process defined in the Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems and the Change Notification Form for Enhanced Direct Enrollment Entities Information Technology Systems located on CMS zONE. This EDE Entity-initiated Change Request process enables an EDE Entity to propose changes to its EDE Environment after it has been audited or approved by CMS with traceability of the changes and an evaluation of the effect of those changes on the EDE Environment. This does not include CMS-initiated CRs (Section XI.B, CMS-initiated Change Requests). The EDE Entity must continue to comply with requirements of the configuration management control family as outlined in the NEE SSP Template.[99] All changes must be tested, validated, and documented before implementing the changes in the production environment.

A primary EDE Entity must submit to CMS an EDE Entity-initiated Change Request to begin the review process of a proposed upstream arrangement prior to onboarding a new prospective upstream EDE Entity, consistent with Section IV.A, Providing an EDE Environment to Other Entities. A primary EDE Entity may submit an EDE Entity-initiated Change Request for a proposed upstream EDE Entity arrangement at any time after the primary and upstream EDE Entities have agreed on the technical implementation and End-user Experience for the EDE Environment, including any proposed additional functionality or systems. Any subsequent changes to the arrangement may require the submission of additional EDE Entity-initiated Change requests. A primary EDE Entity must also submit to CMS an EDE Entity-initiated Change Request, revised ISA Appendix B with changes indicated in the change log, and updated Hub Onboarding Form[100] to remove a previously approved upstream arrangement.

[99] The NEE SSP Template is available on the EDE webpage on CMS zONE: https://zone.cms.gov/document/privacy-and-security-audit.

[100] Upstream EDE Entities may submit the updated Hub Onboarding form directly to CMS rather than the primary EDE Entity. The Hub Onboarding form is available on CMS zONE at the following link: https://zone.cms.gov/document/hub-onboarding-form.

ii. EDE Entity-initiated Phase Change Requests

An EDE Entity-initiated phase change request is a defined subset of modifications that fall under the EDE Entity-initiated CR process. If a prospective phase change EDE Entity opts to change to a different EDE application phase (from its approved or audited EDE phase), the prospective phase change EDE Entity must follow the processes outlined in Section XI.A.i, EDE Entity-initiated Change Request, to submit an EDE Entity-initiated Change Request form with its notice of intent to conduct a phase change audit. After a prospective phase change EDE Entity receives CMS approval to proceed with the phase change audit, the Auditor must conduct portions of a revised business requirements audit to account for the changes to the prospective phase change EDE Entity's EDE environment necessary to implement the newly selected phase and to confirm compliance with all applicable EDE requirements. CMS will review business requirements audit submissions from prospective phase change EDE Entities as if they were initial audit submissions. Any phase change business requirements audit submissions must be received during an audit submission window, as outlined in Section X.B, Audit Submission, and must comply with the audit completeness criteria in Section X.C.i, Submitting a Complete Business Requirements Audit (as applicable to the requirements in Exhibit 11).

Exhibit 11 indicates the required materials a prospective phase change EDE Entity must have an Auditor complete for the business requirements audit for a prospective phase change EDE Entity to be approved by CMS to operate a new application phase.

Exhibit 11: Business Audit Phase Change Requirements

Business Audit Documentation	Business Audit Phase Change Requirements
EDE Business Requirements Audit Instructions and Report Template	▪ For all phase CRs, the prospective phase change EDE Entity's Auditor must document compliance with the business review categories (and the associated toolkits): – Phase-dependent Screener Questions (EDE Phase 2 EDE Entities Only) (if applicable) – Accurate and Streamlined Eligibility Application User Interface (UI) – Post-eligibility Application Communications – Accurate Information about the Exchange and Consumer Communications – Eligibility Results Testing and SES Testing – API Functional Integration Requirements – Application UI Validation – Section 508-compliant UI – Non-English-language Version of the Application UI and Communication Materials (if applicable) – Health Reimbursement Arrangement (HRA) Offer Required UI Messaging (if applicable)
Application UI Toolkit	▪ For all phase CRs, the prospective phase change EDE Entity's Auditor must complete the entirety of the Application UI Toolkit for the EDE Entity's new phase. This includes the screening questions tabs (for Phase 2 EDE Entities only), the UI Questions tab, the High-Level Requirements tab, and the Eligibility Results tab.
Eligibility Results Toolkit	▪ For all phase CRs, the prospective phase change EDE Entity's Auditor must complete all of the relevant test cases for the applicable EDE Entity's phase. For example, if an EDE Entity is changing to Phase 3, the Auditor must complete and submit evidence for all test cases, as noted in the "Auditor User Guide" tab, including the documentation for the applicable test cases in the Phase 2 Eligibility Results Toolkit.

Business Audit Documentation	Business Audit Phase Change Requirements
Communications Toolkit	▪ For phase changes the prospective phase change EDE Entity's Auditor must re-evaluate the compliance of applicable phase-specific requirements as defined in the Communications Toolkit. Phase-specific requirements are clearly and expressly identified in the Communications Toolkit.
API Functional Integration Toolkit	▪ For all phase CRs, the prospective phase change EDE Entity's Auditor must complete all test cases within the API Functional Integration Toolkit.
Other Requirements, as determined by CMS	▪ EDE Entity is required to submit security and privacy impact analysis. ▪ Depending on the prospective phase change EDE Entity's proposed implementation for the phase change, CMS may require additional evidence from the prospective phase change EDE Entity and the Auditor. – For example, if the prospective phase change EDE Entity proposes to also add an upstream EDE Entity as part of the phase change request, CMS may require verification of the appropriate ID proofing requirements for agents, brokers, and consumers. – CMS may require EDE Entities assess additional controls as part of its annual Privacy and Security audit, as described in Section III.A.ii, Privacy and Security Audit.

B. CMS-initiated Change Requests

i. CMS-initiated Change Request Process

CMS will periodically release updates to EDE program requirements in the form of CMS-initiated CRs; these CMS-initiated CRs are documented in the EDE Change Request Tracker.[101] Usually, these changes will take the form of an update to one of the business report toolkits. CMS may require EDE Entities to implement new or updated EDE requirements, including updates to business requirements audit toolkit versions that are released after the date of the CMS-designated baseline version of each toolkit. These required revisions will be considered CMS-initiated CRs. EDE Entities have two options to implement required revisions:

- Submit supplemental documentation; or
- Have their Auditor review the required revision as part of the business requirements audit. For example, if the required revision is in a toolkit, the Auditor will use the version of the toolkit containing the revision(s) to complete the business requirements audit.

All EDE Entities participating in EDE must implement CMS-initiated CRs. However, depending on when an EDE Entity submits its business requirements audit in relation to when CMS notifies EDE Entities about a required CR, the CR may be audited as part of the business requirements audit or the EDE Entity may demonstrate that it has implemented the CR as part of a separate process. Specifically:

- EDE Entities that have already submitted their business requirements audit before the CR is released must submit evidence of their implementation of the CR in clearly labeled supplemental documentation, rather than have their Auditor re-review the portion of the audit affected by the CR.

[101] The EDE Change Request Tracker is located on CMS zONE: https://zone.cms.gov/document/business-audit.

- EDE Entities that submit their audits after the CR is released, but before the implementation deadline have two options: (1) they may have their Auditor review the CR as part of the business requirements audit or (2) they may provide clearly labeled supplemental documentation of their implementation of the CR anytime up until the implementation deadline stated in the EDE Change Request Tracker (explained below).
- EDE Entities that submit their audits after the CR implementation deadline will be required to submit documentation of their implementation of the CR with their audit submission (either incorporated in the Auditor's review or in clearly labeled supplemental documentation).

ii. CMS Change Request Tracker

CMS will specify the changes that EDE Entities are required to implement via the EDE Change Request Tracker, which is posted on CMS zONE.[102]

The EDE Change Request Tracker is a spreadsheet containing information about each CMS-initiated CR, including a description of each CR; the EDE document in which the CR appears; whether the EDE Entity must submit documentation to demonstrate compliance and, if so, the type of documentation the EDE Entity must submit (e.g., if EDE Entities must submit screenshots or some other type of evidence of implementation); the deadline for submission of documentation; the method of submission of required documentation; and conditional requirements, if applicable. The Change Request Tracker only describes the CR; the EDE Entity must review the CR within the identified EDE document.

iii. Deadlines for Implementation of Required Changes and Potential Penalties

CMS will attempt to provide as much notice to EDE Entities as feasible regarding CMS-initiated CRs. Per the EDE Business Agreement, CMS will provide a timeline for each CMS-initiated CR for EDE Entities to implement the change. Prospective EDE Entities must submit supplemental evidence of implementation of CMS-initiated CRs that have passed the deadline for submission prior to EDE approval. While CMS anticipates that this will be a rare occasion, some CMS-initiated CRs may require significant revisions to the EDE environment that would require independent verification by a third-party Auditor. CMS will attempt to provide more advance notice to EDE Entities in the event CMS requires a CMS-initiated CR of this type.

If an EDE Entity does not timely submit documentation of its implementation of such CRs, CMS may suspend the non-compliant EDE Entity's access to the EDE pathway. If an EDE Entity does not meet the deadline to provide evidence of implementation of the CR and has not already been approved to participate in EDE, the EDE Entity will not be approved until after the appropriate documentation is submitted.

iv. Implementation of Other Changes

CMS will periodically release updates to EDE documentation that are not included in the Change Request Tracker. These updates include clarifications, technical corrections, and content updates. These types of updates do not amount to changes in business requirements and accordingly will not be communicated through the Change Request Tracker. Instead, these changes will be noted

[102] The EDE Change Request Tracker is located on CMS zONE: https://zone.cms.gov/document/business-audit.

through release of new versions of EDE documentation and communicated through EDE partner calls, e-blasts, and other technical assistance channels.

While proof of implementation is not required for this category of changes, EDE Entities are strongly encouraged to pay close attention to and implement these updates where appropriate, as failure to do so may result in validation or other errors or have other adverse impacts on an EDE Entity's environment.

If an EDE Entity is making a change to its EDE environment consistent with this subsection, the EDE Entity must review the Change Notification Procedures for Enhanced Direct Enrollment Entity Information Technology Systems document consistent with Section XI.A.i, EDE Entity-initiated Change Request Process.

C. Retiring or Decommissioning the EDE Environment

The evolution of business needs and technology may result in obsolete and inadequate IT systems that need to be retired and decommissioned. The decommissioning, data retention, and data disposition activities ensure the orderly decommissioning of the NEE IT systems and the preservation of vital information about those systems. CMS has established the *Decommissioning Plan for Non-Exchange Entities (NEEs)* to minimize risks and negative impacts associated with decommissioning of the IT systems. An EDE Entity must reference and complete the NEE Decommissioning Plan and NEE Decommissioning Close Out Letter in situations where the EDE Entity will retire or decommission its EDE environment.[103]

Consistent with Section V, Termination, of the EDE Business Agreement, an EDE Entity must provide thirty (30) Days' prior written notice to terminate its Agreement with CMS. This written notice must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents. Additionally, the EDE Entity must also provide written notice to its subscribers no less than ten (10) days prior to the date of termination and must prominently display notification of termination on its website as well as instructions on how to access the application.

XII. Resources

A. Help Desk

In addition to hosting weekly webinars inclusive of interactive question and answers, CMS currently manages multiple EDE Entity-facing help desks to address questions; help EDE Entities and prospective EDE Entities resolve technical problems, operational issues, and other issues, and respond to policy questions. An Entity must either remove PII in documents before sending them to the help desks or encrypt the e-mail transmitting the PII.

- An EDE Entity with technical issues or questions that concern its technical build or system issues identified in the test or production environment should email both CMS.FFE.EDESupport@afs.com and CMS_FEPS@cms.hhs.gov with the subject line

[103] The *Non-Exchange Entity (NEE) Decommissioning Plan* and *NEE Decommissioning Close Out Letter* are available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit
.

"EDE: Tech Q for [Partner] on [Topic]." An EDE Entity may also use the same Help Desks to send technical questions asked by its Auditor(s).

- An EDE Entity with technical questions related to Hub access or connectivity with any of the EDE APIs or services, or with questions about testing or approval to use the RIDP/FARS services should email both Hubsupport@sparksoftcorp.com and CMS_FEPS@cms.hhs.gov with the subject line "EDE: Tech Q for [Partner] on [Topic]." An EDE Entity may also use the same Help Desks to send related questions asked by its Auditor(s).
- An EDE Entity that wishes to integrate with the Marketplace API suite, which includes various plan data services, can find related documentation at https://developer.cms.gov/marketplace-api/ and can send questions related to integration to marketplace-api@cms-provider-directory.uservoice.com with the subject line "EDE: MAPI Q for [Partner] on [Topic]."

For a timely response, the EDE Entity representative submitting the question should ensure that emails to the Help Desks include the following information:

- Your contact information (e-mail and phone number).
- Name of your organization and either your organization's five-character Health Insurance Oversight System (HIOS) ID (if an existing issuer) or CMS-issued Partner ID (if an existing web-broker).
- At the top of your email, please summarize whether your e-mail concerns an EDE technical question, testing issue, or production issue, where possible. Additionally, please note the environment where the issue was encountered, if applicable. This summary will enable the Help Desk to route the email to the right Subject Matter Expert (SME) for a more efficient response.
- If reporting on a technical issue you encounter in production or while testing EDE, please include the request/response XMLs/JSONs (API requests and responses) for troubleshooting when applicable. If the XMLs/JSONs include PII, EDE Entities must remove PII prior to sending the XMLs/JSONs to the Help Desks or the EDE Entity must encrypt the email.

An EDE Entity with a policy or compliance question related to the business requirements audit or EDE Business Agreement should email DE Support at directenrollment@cms.hhs.gov.

An EDE Entity with a policy or compliance question related to the privacy and security audit, privacy and security controls, or its ISA should email DE Support at directenrollment@cms.hhs.gov.

CMS may not respond to policy questions on either of these topics if they are not sent to DE Support.

An EDE Entity with an eligibility application requirements and/or eligibility application UI flexibility question should email DE Support at directenrollment@cms.hhs.gov.

CMS will summarize and share answers to frequently asked questions (FAQs) on EDE that are sent to DE Support on the CMS-Issuer Technical Work Group (ITWG) webinar, which is open to all issuers and web-brokers on Tuesday afternoons. Not all workgroup content is relevant to

EDE Entities, but CMS strongly recommends that EDE Entities attend these calls to hear important announcements, updates, reminders, and clarifications. Please see the Section XII.C, Webinars, for webinar details.

B. Office Hours

CMS will host office hours throughout the year. During these office hours, CMS will aim to provide targeted, detailed technical assistance to prospective and existing EDE Entities and their Auditors. These office hours have limited availability and will be assigned on a first-come, first-served basis. CMS will not schedule office hour sessions to discuss standard help desk inquiries that can be resolved through DE Support. EDE Entities should submit requests for office hours to DE Support (directenrollment@cms.hhs.gov).

C. Webinars

CMS currently hosts the ITWG webinar on Tuesdays from 3:00 PM to 4:30 PM ET. The schedule adjusts throughout the year. Please refer to the registration URL below for more information. The ITWG call is open to all web-brokers and issuers operating on the FFE or SBE-FPs. CMS will continue to use the ITWG call to update the DE/EDE community on developments related to EDE and offer interactive question and answer time at the end of each session.

To obtain the call-in information for the weekly ITWG webinar, users must register via a one-time Webinar Registration URL for the ITWG meeting series. This URL can be found on CMS zONE.[104]

For all webinars, CMS will make the slides available during or shortly after the presentation. CMS will advertise and update logistical information (dates/times, dial-in numbers, and webinar URLs) on the CMS zONE Private Issuer Community and Web-Broker Community webpage.

D. CMS zONE Communities (Guidance & Technical Resources)

CMS currently posts all technical information, guidelines, such as those referenced in this document, as well as webinar slide decks, audit resources, and other documentation on the CMS zONE EDE webpage.[105] CMS has divided these pages and the documentation across the following subject areas: General EDE Guidance and Information, Business Audit Resources, Privacy and Security Audit Resources, Eligibility Information, API Information, EDE Slides From Issuer Technical Workgroup, Upcoming and Historical Deployment Information, and Additional Direct Enrollment Information.

This webpage is accessible by members of the following CMS zONE communities: Private Issuer Community (for issuers), the Web-Broker Community (for web-brokers), and the EDE Auditors Community.[106] CMS will post all EDE updates, information for third-party Auditors,

[104] Webinar Registration can be found at the following link on CMS zONE: https://cms.zoomgov.com/webinar/register/WN_RXkO5638StCAdE-RNESWpg.

[105] Generally, EDE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment.

[106] Once CMS receives a copy of the Auditor's contract with a primary EDE Entity, CMS will send a copy of the instructions to access CMS zONE to the primary EDE Entity for sharing with the Auditor.

webinar slide decks, and FAQs to these communities, and will highlight updates during the weekly ITWG webinars.

CMS will provide updates with further requirements and resources as they become available. A prospective EDE Entity should regularly check the EDE webpage. Unless otherwise specified, any guidance or requirements stated as forthcoming in this document are expected to be made available through the CMS zONE Communities for EDE.

E. REGTAP

CMS will make the trainings and a list of essential EDE resources available via REGTAP.[107]

F. Additional Guidance

- Federally-facilitated Exchanges (FFEs) Enrollment Manual: https://www.cms.gov/files/document/ffe-enrollment-manual-2023-5cr-071323.pdf
- Updated Web-broker Direct Enrollment Program Participation Minimum Requirements: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/2020-WB-Program-Guidance-052120-Final.pdf
- For a current list of states that run their own State-based Exchange and do not use the Federal Platform, visit https://www.healthcare.gov/marketplace-in-your-state/. EDE Entities can use this list with state website links to refer consumers or agents/brokers in these states to their state's website
  - **Note:** Some states listed use the Federal Platform (HealthCare.gov) for individual coverage but run their own SHOP coverage operations. CMS will provide information to EDE Entities if changes are made in the future.
- Privacy Act of 1974: http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/PrivacyActof1974.html
- The Current Acceptable Risk Safeguards (ARS) documentation: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication
- CCIIO Regulations and Standards: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/index.html
- HHS Guidance Submissions: https://www.hhs.gov/guidance/
- CMS Risk Management Handbook (RMH) Chapter 08: Incident Response: https://www.cms.gov/files/document/rmh-chapter-08-incident-response.pdf

[107] REGTAP can be accessed at the following link: https://www.regtap.info/.

Appendix A. Privacy and Security Controls for Hybrid Non-issuer Upstream EDE Entities

Exhibit 12 and Exhibit 13 in this Appendix apply to hybrid non-issuer upstream EDE Entities as described in Section IV.A.iv, Privacy and Security Audit Requirements for Hybrid Non-issuer Upstream EDE Entities. Exhibit 14 applies to the hybrid issuer upstream EDE Entities as described in Section IV.A.v, Privacy and Security Audit Requirements for Hybrid Issuer Upstream EDE Entities Implementing Single Sign-On. The full list of privacy and security controls that apply to primary EDE Entities are documented in the NEE System Security Plan (SSP) Template and the EDE Streamlined Subset NIST 800-53 controls[108] documents on CMS zONE.[109]

The hybrid non-issuer upstream EDE Entity's Auditor must evaluate the EDE Entity's compliance with the EDE privacy and security controls documented in Exhibit 12 (as applicable to the arrangement).

Exhibit 12: Auditable (Non-Inheritable and Hybrid) Controls

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
Access Control (AC)			
AC-1	Access Control Policy and Procedures	-	X
AC-2	Account Management	-	X
AC-2(1)	Automated System Account Management	-	X
AC-2(2)	Removal of Temporary/Emergency Accounts	-	X
AC-2(3)	Disable Inactive Accounts	-	X
AC-2(4)	Automated Audit Actions	-	X
AC-2(7)	Role-Based Schemes	-	X
AC-2(10)	Shared / Group Account Credential Termination	-	X
AC-5	Separation of Duties	-	X
AC-18	Wireless Access	X	-
AC-18(1)	Authentication and Encryption	X	-
AC-19	Access Control for Mobile Devices	X	-
AC-19(5)	Full-Device / Container-Based Encryption	X	-
AC-20	Use of External Information Systems	X	-
AC-20(1)	Limits on Authorized Use	X	-
AC-20(2)	Portable Storage Devices	X	-
AC-21	Information Sharing	X	-
AC-22	Publicly Accessible Content	X	-
Awareness and Training (AT)			
AT-1	Security Awareness and Training Policy and Procedures	X	
AT-2	Security Awareness Training	X	
AT-2(2)	Insider Threat	X	

[108] The current NEE SSP controls are based on NIST SP 800-53 Rev. 4.

[109] These files are available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
AT-3	Role-Based Security Training	X	
AT-4	Security Training Records	X	
Audit and Accountability (AU)			
AU-1	Audit and Accountability Policy and Procedures	X	
AU-2	Audit Events		X
AU-2(3)	Reviews and Updates		X
AU-6	Audit Review, Analysis, and Reporting		X
AU-6(1)	Process Integration		X
AU-6(3)	Correlate Audit Repositories		X
AU-7	Audit Reduction and Report Generation		X
AU-7(1)	Automatic Processing		X
AU-8	Time Stamps		X
AU-8(1)	Synchronization with Authoritative Time Source		X
AU-9	Protection of Audit Information		X
Security Assessment and Authorization (CA)			
CA-1	Security Assessment and Authorization Policies and Procedures		X
CA-2	Security Assessments		X
CA-2(1)	Independent Assessors		X
CA-3(5)	Restrictions on External System Connections	X	
CA-5	Plan of Action and Milestones	X	
CA-6	Security Authorization		X
CA-7	Continuous Monitoring	X	
CA-7(1)	Independent Assessment	X	
CA-9	Internal System Connections	X	
Configuration Management (CM)			
CM-1	Configuration Management Policy and Procedures		X
CM-2	Baseline Configuration		X
CM-2(1)	Reviews and Updates		X
CM-2(3)	Retention of Previous Configurations		X
CM-3	Configuration Change Control	X	
CM-3(2)	Test/Validate/Document Changes	X	
CM-4	Security Impact Analysis	X	
CM-4(1)	Separate Test Environments	X	
CM-9	Configuration Management Plan		X
Contingency Planning (CP)			
CP-2	Contingency Plan		X
CP-2(1)	Coordinate with Related Plans	X	
CP-2(3)	Resume Essential Missions/Business Functions	X	
CP-2(8)	Identify Critical Assets	X	
CP-3	Contingency Training	X	

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
CP-4	Contingency Plan Testing	X	
CP-4(1)	Coordinate with Related Plans	X	
CP-8	Telecommunications Services		X
CP-8(1)	Priority of Service Provisions		X
CP-8(2)	Single Points of Failure		X
CP-9	Information System Backup	X	
CP-9(1)	Testing for Reliability/Integrity	X	
CP-10	Information System Recovery and Reconstitution		X
CP-10(2)	Transaction Recovery		X
Identification and Authentication (IA)			
IA-1	Identification and Authentication Policy and Procedures	X	
Incident Response (IR)			
IR-1	Incident Response Policy and Procedures	X	
IR-2	Incident Response Training	X	
IR-3	Incident Response Testing	X	
IR-3(2)	Coordination with Related Plans	X	
IR-4	Incident Handling	X	
IR-4(1)	Automated Incident Handling Processes	X	
IR-5	Incident Monitoring	X	
IR-6	Incident Reporting	X	
IR-6(1)	Automated Reporting	X	
IR-7	Incident Response Assistance	X	
IR-7(1)	Automation Support for Availability of Information/Support	X	
IR-8	Incident Response Plan	X	
IR-9	Information Spillage Response	X	
Media Protection (MP)			
MP-1	Media Protection Policy and Procedures		X
MP-2	Media Access		X
MP-3	Media Marking		X
MP-4	Media Storage		X
MP-5	Media Transport		X
MP-5(4)	Cryptographic Protection		X
MP-6	Media Sanitization		X
MP-7	Media Use		X
MP-7(1)	Prohibit Use Without Owner		X
Physical and Environmental Protection (PE)			
PE-1	Physical and Environmental Protection Policy and Procedures		X
PE-2	Physical Access Authorizations		X
PE-2(1)	Access by Position / Role		X
PE-3	Physical Access Control		X

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
PE-4	Access Control for Transmission Medium		X
PE-5	Access Control for Output Devices		X
PE-6	Monitoring Physical Access		X
PE-6(1)	Intrusion Alarms/Surveillance Equipment		X
PE-8	Visitor Access Records		X
Planning (PL)			
PL-1	Security Planning Policy and Procedures		X
PL-2	System Security Plan		X
PL-2(3)	Plan/Coordinate with Other Organizational Entities		X
PL-4	Rules of Behavior		X
PL-4(1)	Social Media and Networking Restrictions		X
PL-8	Information Security Architecture		X
Personnel Security (PS)			
PS-1	Personnel Security Policy and Procedures	X	
PS-2	Position Risk Designation	X	
PS-3	Personnel Screening	X	
PS-4	Personnel Termination	X	
PS-5	Personnel Transfer	X	
PS-6	Access Agreements	X	
PS-7	Third-Party Personnel Security	X	
PS-8	Personnel Sanctions	X	
Risk Assessment (RA)			
RA-1	Risk Assessment Policy and Procedure		X
RA-3	Risk Assessment		X
RA-5	Vulnerability Scanning		X
System and Services Acquisition (SA)			
SA-5	Information System Documentation		X
System and Communications Protection (SC)			
SC-28	Protection of Information at Rest	X	
SC-CMS-1	Electronic mail	X	
Accountability, Audit, and Risk Management (AR)			
AR-1	Governance and Privacy Program		X
AR-2	Privacy Impact and Privacy Program		X
AR-4	Privacy Monitoring and Auditing		X
AR-5	Privacy Awareness and Training	X	
AR-8	Accounting of Disclosures	X	
Data Quality and Integrity (DI)			
DI-1	Data Quality		X
DI-1(1)	Validate PII	X	

Control #	Security/Privacy Control Name	Non-Inheritable Controls	Hybrid Controls
Data Minimization and Retention (DM)			
DM-3	Minimization of PII Used in Testing, Training, and Research		X
DM-3 (1)	Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques		X
Individual Participation and Redress (IP)			
IP-1	Consent		X
IP-2	Individual Access		X
IP-3	Redress		X
IP-4	Complaint Management		X
IP-4(1)	Complaint Management/Response Times		X
Security (SE)			
SE-1	Inventory of Personally Identifiable Information		X
SE-2	Privacy Incident Response		X
Transparency (TR)			
TR-1	Privacy Notice		X
TR-3	Dissemination of Privacy Program Information		X
Use Limitation (UL)			
UL-1	Internal Use	X	
UL-2	Information Sharing with Third Parties	X	

Exhibit 13 reflects the Inheritable Common Controls that the hybrid non-issuer upstream EDE Entity can potentially inherit from the primary EDE Entity. The hybrid non-issuer upstream EDE Entity's Auditor does not need to independently evaluate the implementation of any inherited common controls implemented by the approved primary EDE Entity.

Exhibit 13: Inheritable Common Controls

Control #	Security/Privacy Control Name
Access Control (AC)	
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-6	Least Privilege
AC-6(1)	Authorize Access to Security Functions
AC-6(2)	Non-Privileged Access for Non-Security Functions
AC-6(5)	Privileged Accounts
AC-6(9)	Auditing Use of Privileged Functions
AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions
AC-7	Unsuccessful Logon Attempts
AC-8	System Use Notification
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-11(1)	Pattern-Hiding Displays
AC-12	Session Termination
AC-14	Permitted Actions Without Identification or Authentication
AC-17	Remote Access
AC-17(1)	Automated Monitoring/Control
AC-17(2)	Protection of Confidentiality/Integrity Using Encryption
AC-17(3)	Managed Access Control Points
AC-17(4)	Privileged Commands/Access
AC-17(9)	Disconnect / Disable Access
Audit and Accountability (AU)	
AU-3	Content of Audit Records
AU-3(1)	Additional Audit Information
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-5(1)	Audit Storage Capacity
AU-9(4)	Access by Subset of Privileged Users
AU-10	Non-Repudiation
AU-11	Audit Record Retention
AU-12	Audit Generation
Security Assessment and Authorization (CA)	
CA-3	System Interconnections
CA-8	Penetration Testing
CA-8(1)	Independent Penetration Agent or Team

Control #	Security/Privacy Control Name
Configuration Management (CM)	
CM-5	Access Restrictions for Change
CM-5(1)	Automated Access Enforcement/Auditing
CM-5(5)	Limit Production/Operational Privileges
CM-6	Configuration Settings
CM-6(1)	Automated Central Management/ Application/Verification
CM-7	Least Functionality
CM-7(1)	Periodic Review
CM-7(2)	Prevent Program Execution
CM-7(4)	Unauthorized Software/Blacklisting
CM-8	Information System Component Inventory
CM-8(1)	Updates During Installations/Removals
CM-8(3)	Automated Unauthorized Component Detection
CM-8(5)	No Duplicate Accounting of Components
CM-10	Software Usage Restrictions
CM-10(1)	Open Source Software
CM-11	User-Installed Software
Contingency Planning (CP)	
CP-1	Contingency Planning Policy and Procedures
CP-2(2)	Capacity Planning
CP-6	Alternate Storage Site
CP-6(1)	Separation from Primary Site
CP-6(3)	Accessibility
Identification and Authentication (IA)	
IA-2	Identification and Authentication (Organizational Users)
IA-2(1)	Network Access to Privileged Accounts
IA-2(2)	Network Access to Non-Privileged Accounts
IA-2(3)	Local Access to Privileged Accounts
IA-2(8)	Network Access to Privileged Accounts – Replay Resistant
IA-2(11)	Remote Access – Separate Device
IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-5(1)	Password-Based Authentication
IA-5(2)	PKI-Based Authentication
IA-5(3)	In-Person or Trusted Third-Party Registration
IA-5(7)	No Embedded Unencrypted Static Authenticators
IA-5(11)	Hardware Token-Based Authentication
IA-6	Authenticator Feedback
IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non-Organizational Users)

Control #	Security/Privacy Control Name
IA-8(2)	Acceptance of Third-Party Credentials
Maintenance (MA)	
MA-1	System Maintenance Policy and Procedures
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-3(1)	Inspect Tools
MA-3(2)	Inspect Media
MA-3(3)	Prevent Unauthorized Removal
MA-4	Nonlocal Maintenance
MA-4(1)	Auditing and Review
MA-4(2)	Document Nonlocal Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
Risk Assessment (RA)	
RA-5(1)	Update Tool Capability
RA-5(2)	Update by Frequency/Prior to New Scan/When Identified
RA-5(5)	Privileged Access
System and Services Acquisition (SA)	
SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	System Development Life Cycle
SA-4	Acquisition Process
SA-4(1)	Functional Properties of Security Controls
SA-4(2)	Design/Implementation Information for Security Controls
SA-4(9)	Functions/Ports/Protocols/Services in Use
SA-8	Security Engineering Principles
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing and Evaluation
SA-15	Development Process, Standards, and Tools
SA-17	Developer Security Architecture and Design
SA-22	Unsupported System Components
System and Communications Protection (SC)	
SC-1	System and Communications Protection Policy and Procedures
SC-2	Application Partitioning
SC-4	Information in Shared Resources
SC-5	Denial of Service Protection
SC-6	Resource Availability
SC-7	Boundary Protection
SC-7(3)	Access Points
SC-7(4)	External Telecommunications Services

Control #	Security/Privacy Control Name
SC-7(5)	Deny by Default/Allow by Exception
SC-7(7)	Prevent Split Tunneling for Remote Devices
SC-7(8)	Route Traffic to Authenticated Proxy Servers
SC-7(12)	Host-Based Protection
SC-7(13)	Isolation of Security Tools/Mechanisms/Support Components
SC-7(18)	Fail Secure
SC-8	Transmission Confidentiality and Integrity
SC-8(1)	Cryptographic or Alternate Physical Protection
SC-8(2)	Pre/Post Transmission Handling
SC-10	Network Disconnect
SC-12	Cryptographic Key Establishment and Management
SC-12(2)	Symmetric Keys
SC-13	Cryptographic Protection
SC-17	Public Key Infrastructure Certificates
SC-18	Mobile Code
SC-19	Voice Over Internet Protocol
SC-20	Secure Name/Address Resolution Service (Authoritative Source)
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Name/Address Resolution Service
SC-23	Session Authenticity
SC-24	Fail in Known State
System and Information Integrity (SI)	
SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-2(2)	Automated Flaw Remediation Status
SI-2(3)	Time to Remediate Flaws / Benchmarks for Corrective Actions
SI-3	Malicious Code Protection
SI-3(2)	Automatic Updates
SI-4	Information System Monitoring
SI-4(1)	System-Wide Intrusion Detection System
SI-4(4)	Inbound and Outbound Communications Traffic
SI-4(5)	System-Generated Alerts
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security Function Verification
SI-7	Software, Firmware, and Information Integrity
SI-7(1)	Integrity Checks
SI-7(7)	Integration of Detection and Response
SI-8	Spam Protection
SI-8(2)	Automatic Updates
SI-10	Information Input Validation
SI-11	Error Handling

Control #	Security/Privacy Control Name
SI-12	Information Handling and Retention
SI-16	Memory Protection
Authority and Purpose (AP	
AP-1	Authority to Collect
AP-2	Purpose Specification
Accountability, Audit, and Risk Management (AR)	
AR-7	Privacy-enhanced System Design and Development
Data Minimization and Retention (DM)	
DM-1	Minimization of Personally Identifiable Information
DM-1(1)	Minimization of PII/Locate/Remove/Redact/Anonymize PII
DM-2	Data Retention and Disposal
DM-2 (1)	Data Retention and Disposal/System Configuration

The Auditor for Hybrid Issuer Upstream EDE Entities Implementing Single Sign-On must evaluate the Entity's compliance with the privacy and security controls listed in Exhibit 14.

Exhibit 14: Auditable Controls for Hybrid Issuer Upstream EDE Entities Implementing Single Sign-On

Control #	Security/Privacy Control Name
Access Control (AC)	
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-2(1)	Account Management | Automated System Account Management
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts
AC-2(3)	Account Management | Disable Inactive Accounts
AC-2(4)	Account Management | Automated Audit Actions
AC-2(7)	Account Management | Termination Role-Based Schemes
AC-2(10)	Account Management | Shared / Group Account Credential Termination
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-6(1)	Least Privilege | Authorize Access to Security Functions
AC-6(2)	Least Privilege | Non-Privileged Access for Non-Security Functions
AC-6(5)	Least Privilege | Privileged Accounts
AC-6(9)	Least Privilege | Auditing Use of Privileged Functions
AC-6(10)	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions
AC-7	Unsuccessful Logon Attempts
AC-8	System Use Notification
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-11(1)	Session Lock | Pattern-Hiding Displays
AC-12	Session Termination
AC-14	Permitted Actions Without Identification or Authentication
AC-17	Remote Access
AC-17(1)	Remote Access | Automated Monitoring/Control
AC-17(2)	Remote Access | Protection of Confidentiality / Integrity Using Encryption
AC-17(3)	Remote Access | Managed Access Control Points
AC-17(4)	Remote Access | Privileged Commands / Access
AC-17(9)	Remote Access | Disconnect / Disable Access
AC-18	Wireless Access
AC-18(1)	Wireless Access | Authentication and Encryption
AC-19	Access Control for Mobile Devices
AC-19(5)	Access Control for Mobile Devices | Full-Device / Container-Based Encryption
AC-20	Use of External Information Systems
AC-20(1)	Use of External Information Systems | Limits on Authorized Use

Control #	Security/Privacy Control Name
AC-20(2)	Use of External Information Systems | Portable Storage Devices
AC-21	Information Sharing
AC-22	Publicly Accessible Content
Awareness and Training (AT)	
AT-2(2)	Security Awareness Security Awareness Training | Insider Threat
AT-3	Role-Based Security Training
Audit and Accountability (AU)	
AU-1	Audit and Accountability Policy and Procedures
AU-2	Audit Events
AU-3	Content of Audit Records
AU-6	Audit Review, Analysis, and Reporting
AU-8	Time Stamps
AU-11	Audit Record Retention
Security Assessment and Authorization (CA)	
CA-2	Security Assessments
CA-3	System Interconnections
CA-5	Plan of Action and Milestones
CA-7	Continuous Monitoring
CA-8	Penetration Testing
Configuration Management (CM)	
CM-2	Baseline Configuration
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-6	Configuration Settings
CM-7	Least Functionality
Identification and Authentication (IA)	
IA-1	Identification and Authentication Policy and Procedures
IA-2	Identification and Authentication (Organizational Users)
IA-2(1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts
IA-2(2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts
IA-2(3)	Identification and Authentication (Organizational Users) | Local Access to Privileged Accounts Access to Privileged Accounts
IA-2(8)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts – Replay Resistant
IA-2(11)	Identification and Authentication (Organizational Users) | Remote Access – Separate Device
IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-5(1)	Authenticator Management | Password-Based Authentication
IA-5(2)	Authenticator Management | PKI-Based Authentication
IA-5(3)	Authenticator Management | In-Person or Trusted Third-Party Registration

Control #	Security/Privacy Control Name
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators
IA-5(11)	Authenticator Management | Hardware Token-Based Authentication
IA-6	Authenticator Feedback
IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non-Organizational Users)
IA-8(2)	Acceptance of Third-Party Credentials
Incident Response (IR)	
IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training
IR-4	Incident Handling
IR-6	Incident Reporting
Physical and Environmental Protection (PE)	
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
Planning (PL)	
PL-2	System Security Plan
PL-4	Rules of Behavior
Personnel Security (PS)	
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-6	Access Agreements
Risk Assessment (RA)	
RA-3	Risk Assessment
RA-5	Vulnerability Scanning
System and Services Acquisition (SA)	
SA-4	Acquisition Process
SA-5	Information System Documentation
SA-9	External Information System Services
System and Communications Protection (SC)	
SC-5	Denial of Service Protection
SC-7	Boundary Protection
SC-7(3)	Boundary Protection | Access Points
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers
SC-7(12)	Boundary Protection | Host-Based Protection
SC-8	Transmission Confidentiality and Integrity
SC-10	Network Disconnect
SC-28	Protection of Information at Rest
SC-CMS-1	Electronic Mail
System and Information Integrity (SI)	
SI-2	Flaw Remediation

Control #	Security/Privacy Control Name
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-4(4)	Information System Monitoring | System-Wide Intrusion Detection System
Accountability, Audit, and Risk Management (AR)	
AR-2	Privacy Impact and Risk Assessment
AR-4	Privacy Monitoring and Auditing
Data Minimization and Retention (DM)	
DM-1	Minimization of Personally Identifiable Information
DM-1(1)	Minimization of PII/Locate/Remove/Redact/Anonymize PII
DM-3	Minimization of PII Used in Testing, Training, and Research
Individual Participation and Redress (IP)	
IP-1	Consent
IP-2	Individual Access
IP-4	Complaint Management
Security (SE)	
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
Transparency (TR)	
TR-1	Privacy Notice
TR-3	Dissemination of Privacy Program Information