



Date: June 18, 2014

Subject: Frequently Asked Questions about the Annual Independent External Audit of State-based Marketplaces (SBMs)

Below are frequently asked questions and answers (FAQs) related to the annual independent external audit required for all approved and conditionally-approved State-based Marketplaces (SBMs) by 45 CFT Parts 144, 146, 147, et al. (Program Integrity Rule, Part II). These FAQs will provide SBMs with increased understanding of the purpose and processes associated with the auditing and reporting processes.

Audits: Purpose and Governing Authority

Q1: What is the purpose of the independent external audit?

A1: External audits are a standard practice used by government and private and public sector organizations not only to determine the extent to which an organization adheres to managerial policies, procedures, and requirements but also to ensure accountability in all financial and programmatic activities.

Q2: What authority does the Department of Health and Human Services (HHS), Centers for Medicare and Medicaid Services (CMS) have to require SBMs to provide the results of an independent external audit?

A2: The Program Integrity Rule Part II (PI Reg), 45 CFR 155.1200(c) states,

The State [Marketplace] must engage an independent qualified auditing entity which follows generally accepted governmental auditing standards (GAGAS) to perform an annual independent external financial and programmatic audit and must make such information available to the U.S. Department of Health and Human Services for review.

The regulation also states that the Marketplace will submit to CMS, concurrent with the annual report, the results of the audit along with proposals on how it will remedy any material weakness or significant deficiency.

Q3: Will SBMs, State Partnership Marketplaces (SPMs) and/or Federally-facilitated Marketplaces (FFMs) be required to conduct an independent external audit?

A3: All approved and conditionally-approved SBMs are required to conduct an independent external audit.

Q4: Will CMS conduct its own audit of the SBM in addition to the independent external audit?

A4: CMS maintains the authority and option to conduct its own audit of the SBM if the results of the SBM's independent external audit indicate such action is necessary.

Compliance with Audit Business Standards

Q5: What are the compliance standards for SBMs under the independent external audit requirement?

A5: The auditor chosen by the Marketplace must comply with 45 CFR 155.1200(c). CMS proposes that the SBM engage either a governmental or private independent qualified auditing entity that meets financial accounting standards, generally accepted accounting principles (GAAP), and follows GAGAS, to perform an annual independent external financial and programmatic audit of the SBM.

Q6: May employees of the SBM conduct and complete the independent external audit?

A6: No, the auditor must be autonomous from the Marketplace. However, the preamble to the Program Integrity Regulation states that this requirement may be satisfied through an audit by an independent state-government entity. This entity must be selected to avoid any real or potential perception of conflict of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments of independence.

Financial and Programmatic Audit Requirements

Q7: What financial and programmatic requirements must be addressed by the annual independent external audit?

A7: The independent audit must address the following areas:

1. Accurate accounting of Marketplace receipts and expenditures in accordance with GAAP.
2. Compliance with 45 CFR Part 155.
3. Processes and procedures designed to prevent improper eligibility determinations and enrollment transactions.
4. Identification of errors that resulted in incorrect eligibility determinations.

Q8: What should auditors consider in their reviews to address accurate accounting of Marketplace receipts and expenditures in accordance with GAAP?

A8: Suggested elements for auditors to consider include:

- SBM's financial statements and supporting documentation, including a sampling of receipts and expenditures to ensure accuracy.



- Internal controls and related financial and accounting policies and procedures.
- Policies and procedures related to fraud, waste, and abuse (FWA).
- Policies and procedures related to segregation of duties.
- Contracts, including applicable invoices, proposals, and payment records.

Q9: What specific elements can auditors review to address compliance with 45 CFR 155, Subparts C, D, E, and K?

A9 Auditors should review the requirements set forth in 45 CFR 155, Subparts C, D, E, and K and assess the SBM's compliance with each subpart. Requirements and suggested documentation to review for each subpart are provided below:

PI Reg. Subpart	Suggested Elements to Review
<i>Subpart C—General Functions of the Exchange</i>	• Processes and procedures for privacy and security of navigators. • Processes and procedures for addressing complaints. • Processes and procedures for providing assistance in culturally and linguistic appropriate manner. • Training standards. • Breaches of Security or Privacy by a navigator grantee. • Standards designed to prevent and mitigate any conflicts of interest, financial or otherwise. • Confirmation that assures funding for navigator grants does not come from federal funds. • Privacy and Security Safeguards. • Call center information provided to applicants in plain language and in a manner that is accessible to individuals with disabilities and individuals with limited English proficiency.
<i>Subpart D—Exchange Functions in the Individual Market: Eligibility Determinations for Exchange Participation and Insurance Affordability Programs</i>	• Standard operating procedures (SOPs) and processes for making accurate eligibility determinations in compliance with Federal regulations (including resolution of inconsistencies). • Management review/internal controls associated with the prevention of improper eligibility determinations. • Management review/internal controls associated with the identification of incorrect eligibility determinations. • Management review/internal controls associated with compliance with the requirements regarding confidentiality, disclosure, maintenance, and use of information. • Current and fully executed agreements with other entities specifying their respective responsibilities in connection with eligibility determinations, including (if appropriate) those related to exemptions. • Data and records maintenance relating to eligibility verifications and determinations.



PI Reg. Subpart	Suggested Elements to Review
<i>Subpart E—Exchange Functions in the Individual Market: Enrollment in Qualified Health Plans</i>	• SOPs and processes for making accurate enrollments in compliance with Federal regulations. • Management review/internal controls associated with the prevention of improper enrollment transactions, including processes to ensure that enrollees are receiving accurate advance premium tax credits (APTCs), cost-sharing reductions (CSRs), and premiums (and for correction of any discrepancies). • Compliance with Centers for Medicare & Medicaid Services (CMS)-issued Standard Companion Guides (e.g., ASC X12 820 and 834). • Processes to reconcile enrollment information with qualified health plan (QHP) issuers and CMS no less than on a monthly basis. • Data and records maintenance relating to enrollments.
<i>Subpart K—Exchange Functions: Certification of Qualified Health Plans</i>	• Process for recertification of QHPs. • Process for decertification of QHPs. • Policies and procedures for certification of health plans.

Q10: What can auditors review to address processes and procedures to prevent improper eligibility determinations and enrollment transactions?

A10: Suggested elements to review include:

- Eligibility and enrollment policies and procedures.
- Internal and system controls.
- Results of internal auditing and monitoring of the eligibility and enrollment processes.

Q11: What can auditors review to address identification of errors that resulted in incorrect eligibility determinations?

A11: Suggested elements to review include:

- Eligibility policies and procedures.
- Results of internal auditing and monitoring of the eligibility process.
- Error logs and corrective actions.

Technology, Privacy, and Security Elements

Q12: What technology, privacy, and security controls can auditors review to ensure compliance with the regulatory requirements in 45 CFR Part 155?

A12: To address the technology, privacy and security programmatic requirements of the Independent External Audit, SBMs will need to coordinate with their auditors to establish and implement an annual audit process. The assessment procedures must take into consideration the regulatory requirements and the associated legal agreements that states signed with non-Marketplace entities and with CMS, and ultimately provide the results to HHS.

CMS expects states to establish a program that allows reuse of audits, security reviews, privacy assessments, and other relevant reviews, based on the controls documented in the system security



plan (SSP), to demonstrate a successful and ongoing oversight and monitoring (O&M) program. CMS also expects states to submit the required artifacts to adhere to the Minimum Acceptable Risk Standards for Exchanges (MARS-E) standards (e.g., system security plan, security assessment report, plan of action and milestones, privacy impact assessment).

As the state compliance program matures, CMS expects the ongoing external audits to address the artifacts review that CMS currently performs. Eventually, CMS may elect to rely on the external audit report(s) rather than request separate artifact submissions.

Q13: What are the guiding principles that should be in place to shape privacy and security standards, policies, and supporting procedures?

A13: The table below outlines the principles that must be adhered to when implementing privacy and security standards, as stipulated by 45 CFR 155.260(a)(3).

Principle	Description
<i>Individual Access</i>	Individuals should be provided with a simple and timely means to access and obtain their personally identifiable information (PII) in a readable form and format.
<i>Correction</i>	Individuals should be provided with a timely means to dispute the accuracy or integrity of their PII and to have erroneous information corrected or to have a dispute documented if their requests are denied.
<i>Openness and Transparency</i>	There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their PII.
<i>Individual Choice</i>	Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their PII.
<i>Collection, Use, and Disclosure</i>	PII should be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
<i>Data Quality and Integrity</i>	Persons and entities should take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
<i>Safeguards</i>	PII should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
<i>Accountability</i>	These principles should be implemented, and adherence assured through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

Q14: What type of policies and procedures should be in place to report and respond to an identified privacy or security incident?

A14: Per the MARS-E, each SBM is required to develop and document a set of policies and procedures that serve as the foundation for its incident response program. These policies and procedures must be a written document, approved and signed by management, which addresses the purpose, scope, roles, and responsibilities within the program. Additionally, these documents need to be detailed and ensure consistency and effectiveness based on the unique requirements of the state, which is determined by its size and structure. These policies must be supported by an incident response plan that includes detailed, state-specific procedures for management and staff to follow. Furthermore, as part of its annual assessment process, each state must ensure that management and staff are aware of their roles and responsibilities, and are trained appropriately on a regular basis.

SBMs must report all suspected or confirmed incidents, whether or not they contain Personally Identifiable Information (PII), within one hour of discovery. SBMs must follow the requirements of their legal agreements with CMS. SBMs that connect to the Federal Data Services Hub (FDSH) must sign the Interconnection Security Agreement (ISA), the Computer Matching Agreement (CMA), and the Information Exchange Agreement (IEA). Each written legal agreement has incident reporting requirements that, when combined, require the SBM to report all incidents to CMS. These requirements apply to all system environments (i.e., production, pre-production, test, development). After the initial reporting of an incident, CMS and SBM personnel will continue to work together for the duration of the incident.

Any suspected loss, breach, or misuse of Federal Tax Information (FTI) must be reported within 24 hours to the IRS Office of Safeguards by email to safeguardreports@irs.gov, and by telephone to the Treasury Inspector General for Tax Administration (TIGTA) at 1 (800) 589-3718. An SBM should not wait until its own internal investigation has been conducted to report an incident to CMS, TIGTA, and the IRS.

Q15: If the SBM is sharing data with a third party on a regular basis, what type of agreements should be in place to adhere to privacy and security standards?

A15: The SBM should ensure:

- All agreements bind the other party to meet the requirements specified within 45 C.F.R. 155.260(a)(3) including the ISA, CMA and IEA.
- When providing PII to agencies administering Medicaid or Children's Health Insurance Program (CHIP) programs, the matching and/or sharing arrangements that facilitate the movement of eligibility information must meet the requirements in 45 C.F.R. 155.260, Sections 1413(c)(1) and (c)(2) of the Affordable Care Act (ACA), and Section 1942 of the Social Security Act.
- When interacting with a non-Marketplace entity other than Medicaid/CHIP agencies, such as a Navigator or agent/broker, privacy language must be included within the appropriate agreement required under 45 C.F.R. 155.260(b).

Small Business Health Options Program (SHOP) Standards



Q16: What can auditors review to ensure a SHOP is compliant with the program's standards?

A16: SHOPs must carry out all functions of an Exchange described in subparts C, E, K, and H (with a few exceptions) as well as enrollment and eligibility standards described in 45 C.F.R. 155.710, 155.715, 155.720, 155.725, 155.730, and facilitate the special enrollment periods described in 156.285(b)(2). The table below outlines the guidelines that must be adhered to by a SHOP.

SHOP Guideline	Description
<i>Eligibility Standards</i>	The SHOP is a small employer, or an employer with no less than one employee and no more than 100 employees, unless a State elects to limit enrollment in the small group market to employers with no more than 50 employees until 1/1/16. The SHOP must employ at least one common law employee. An employee would not include a sole proprietor or the sole proprietor's spouse.
<i>Eligibility Determination for SHOP</i>	The SHOP may use the information attested to by the employer or the employee on the application but must, at a minimum verify that an individual attempting to enter the SHOP as an employee is listed on the qualified employer's roster of employees to whom coverage is offered.
<i>Enrollment of Employees into QHPs under SHOP</i>	The SHOP must report to the Internal Revenue Service (IRS) employer participation and employee enrollment information for tax administration purposes.
<i>Enrollment Periods under SHOP</i>	Open enrollment period will be at least 30 days. Employer election period will be at least 30 days. SHOP must establish coverage effective dates consistent with 45 C.F.R. § 155.720.
<i>Application Standard for SHOP</i>	The SHOP must adhere to the application requirements outlined in 45 C.F.R. § 155.730. The SHOP must use a single application to determine employer eligibility and to collect information necessary for purchasing coverage such as employee name and address of employer's locations; number of employees; employer identification number; and list of qualified employees and their taxpayer identification number. The SHOP must use a single application for eligibility determination, QHP selection and enrollment for qualified employees and their dependents. The SHOP may use the model single employer application and model single employee application provided by HHS. The SHOP may also use an alternative application if the application is approved by HHS and meets certain requirements.
<i>Special Enrollment Periods</i>	Special enrollment periods in the SHOP are based on whether an individual becomes a newly eligible qualified employee. Enrollment periods will be available to those who become qualified employees outside of the initial or annual open enrollment period.

Q17: What should be the SHOP policy on non-payment for coverage?

A17: Payment is due on the first of the month. If payment is not received within the 31-day grace period, the SHOP may terminate coverage. To be reinstated, the employer must pay prior premiums owed for coverage during the grace period and pay the premiums for the next month's coverage.

Audit Findings Report

Q18: Based on the financial and programmatic requirements, what type of information should be included in the audit findings report?

A18: The table below outlines suggested topics to include in the audit findings report, as stipulated by CMS and/or GAGAS. This list is not exhaustive, but provides examples of potential content that should be considered during the independent external audit.

Audit Report Topic	Report Content Examples
<i>Executive Summary</i>	• The independent external auditor should include: – Purpose of the audit. – Scope of the audit, including the program areas and time period of the review. – Statement that the auditor has complied with GAGAS audit standards. – Methodology used to conduct the audit to include any quantitative and qualitative tests performed by the auditor. – Nature of confidential or sensitive information that may have been omitted. – General conclusions reached regarding SBM compliance with the financial and programmatic requirements, including compliance with GAAP.
<i>Audit Findings</i>	• The independent external auditor should include: – Specific findings from both the financial and programmatic audits, including a summary of compliance or non-compliance with all requirements. – Material weaknesses, significant deficiencies, and violations found.
<i>Recommendations</i>	• The independent external auditor should include recommended improvements to operating procedures to comply with programmatic and financial requirements. Recommendations should be specific, measurable, attainable, realistic, and time bound.
<i>Conclusion</i>	• The independent external auditor should confirm the firm has reviewed relevant document documentation in compliance with CMS requirements, GAGAS, and GAAP.
<i>Intended Corrective Action Plan</i>	• The SBM should provide detailed corrective action plans on how the Marketplace will address and correct any material weaknesses and significant deficiencies. Details should include rationale and expected completion timeline.

Q19: What format should be used to present the audit findings to CMS?

A19: The audit findings report should be completed in Microsoft Word and provided to CMS as a PDF document. CMS has provided an example template that will comply with the formatting requirements. The example template is available [here](#).

Q20: Is there any additional information that should be obtained from the auditor, in addition to the contents of the audit findings report?

A20: As a requirement of the State-based Marketplace Annual Reporting Tool (SMART), the SBM is required to obtain a signed statement from the auditor with the following information: “An independent, external auditor attests that the Marketplace has demonstrated accurate accounting of all activities, receipts, and expenditures to CMS and prepared an accurate annual financial statement in accordance with GAAP.” This statement must be uploaded as an attachment to the SMART by April 1 of each year.



Audit Findings Report Submission and Timing

Q21: When must the SBM submit the results of the independent external audit to CMS?

A21: Beginning in 2015, the final audit findings report must be completed by April 1 of each year.

Q22: How should an SBM submit the results of the annual external audit to CMS?

A22: A PDF version of the audit findings report should be submitted as part of the SMART on SERVIS.

Audit Findings Maintenance of Records

Q23: Is there a requirement to retain records of the independent external audit?

A23: Yes. The SBM, its contractors, subcontractors, and agents, as required in the PI Reg., must retain documents reviewed and completed based on the independent external audit for 10 years. Documents include records (whether paper, electronic, or other media) and other evidence of accounting procedures and practices of the SBM. These records must be sufficient and appropriate to respond to any periodic auditing, inspection or investigation of the SBM's financial records or to enable CMS or its designee to appropriately evaluate the SBM's compliance with Federal requirements.

Available Audit Resources

Q24: What guidance and resources are available to SBMs to perform the independent external audit and complete the audit findings report?

A24: The table below provides agency-specific and government-wide resources available to the SBM and the auditor as guidance in performing the independent external audit and completing the audit findings report.

Resource	Use	Location
<i>Generally Accepted Governmental Auditing Standards (GAGAS)</i>	- Framework for conducting high-quality audits with competence, integrity, objectivity, and independence. - For use by auditors of government entities, entities that receive government awards, and other audit organizations performing Yellow Book audits.	http://www.gao.gov/yellowbook/overview
<i>Generally Accepted Accounting Principles (GAAP)</i>	- Authoritative source of GAAP developed by the Federal Accounting Standards Advisory Board (FASAB) for Federal entities. - Pertains to financial statements or other financial data.	http://www.fasab.gov/accounting-standards/authoritative-source-of-gaap/
<i>OMB Circular A-133, Audits of States, Local Governments and Non-</i>	Standards for obtaining consistency and uniformity among Federal agencies for the audit of states, local governments, and nonprofit organizations expending	http://www.whitehouse.gov/sites/default/files/omb/assets/a133/a133_revised_2007.pdf



<i>Profit Organizations).</i>	Federal awards.	
<i>Audit Findings Report Example Template</i>	• Requirements that must be fulfilled by auditor and a sample format for submission. • Sample format for the intended correction action plan that must be submitted to CMS by the SBM.	https://servis.cms.gov/resources/document_detail?doc_detail_id=a6f0075a-9a7f-5be3-8a2c-5316253ae230