National Crime Prevention and Privacy Compact Council

Audit Guide

Compact Council Office
1000 Custer Hollow Road
Clarksburg, WV 26306-0145
compactoffice@leo.gov
www.fbi.gov/about-us/cjis/cc

November 2019
Version 3.2

Table of Contents

Preface **1**

Introduction **2**

Audit Objective **3**

Audit Scope **4**

Audit methodology **5**

- General Audit Methodology Considerations
- Pre-Audit
- Assessment
- Post-Audit

Additional Audit Considerations **10**

- Auditor qualifications and training
- Long-term strategies
- Continuous evaluation

Acronyms **11**

Preface

The National Crime Prevention and Privacy Compact (Compact) Council works in partnership with criminal history record custodians, end users, and policy makers to regulate and facilitate the sharing of complete, accurate, and timely criminal history record information to noncriminal justice users in order to enhance public safety, welfare, and security of society while recognizing the importance of individual privacy rights. This is facilitated in part through the development of resource materials for use in protecting criminal justice information from unauthorized and inappropriate access, collection, maintenance, and disclosure.

The Compact Council Audit Guide was developed in consultation with the FBI's Criminal Justice Information Services Division for use as a resource by those entities responsible for meeting the requirements of the *CJIS Security Policy* for the establishment of audits of noncriminal justice agencies. The Audit Guide is intended to provide policy makers and developers with relevant information regarding baseline considerations for audit programs. It is important to note the guide does not replace existing audit procedures, but rather supplements existing audit guidelines and regulations. In addition, the guide should be considered a "living document" and will be updated on an as-needed basis. Users are encouraged to provide feedback and recommendations for improvements to the information contained in the guide.

Introduction

The establishment of formal audits to ensure compliance with applicable requirements is a vital component of an effective protection strategy. Audits are defined quite simply as methodical examinations and reviews. Performance audits are the most applicable type of audit for planning purposes within the framework of assessing noncriminal justice access to criminal history record information. The U.S. Government Accountability Office in its 2018 revision of *Government Auditing Standards* describes the term "performance audit" as:

> …engagements that provide objective analysis, findings, and conclusions to assist management and those charged with governance and oversight to, among other things, improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability. In a performance audit, the auditors measure or evaluate the subject matter of the audit and present the resulting information as part of, or accompanying, the audit report.

All audits are essentially comprised of three high-level components: objective, scope, and methodology. Each of these components will be addressed in the guide from the overarching perspective of access to criminal history record information for noncriminal justice purposes.

Audit Objective

The objective of an audit is simply defined as what the audit will accomplish and answers questions regarding "why we audit." Audit objectives are in part prescribed by the obligation and authority to conduct audits. With respect to access to CHRI for noncriminal justice purposes, three primary obligations and authorities should be considered:

- Each CSA shall at a minimum triennially audit all noncriminal justice agencies which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies. In addition, each CSA shall, in coordination with the SIB, establish a process to periodically audit all noncriminal justice agencies with access to CJI in order to ensure compliance with applicable statutes, regulations and policies. (*CJIS Security Policy, Version 5.8, Section 5.11.2*)

- Each Compact State shall appoint a Compact Officer who shall: administer the Compact within the State; ensure that Compact provisions and rules, procedures, and standards established by the Council are complied with in the State; regulate the in-State use of records received by means of the III System from the FBI or from other Party States; and establish procedures to protect the accuracy and privacy of these records. (*Title 34, United State Code (U.S.C.), Section 40316, Articles III (b) and IV (c)*)

- A Compact Officer/Chief Administrator may not grant permission to outsource an administrative function involving access to CHRI unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. (*Security and Management Control Outsourcing Standards for Channelers and for Non-Channelers, Footnote 2*)

Based on these primary obligations and authorities, decision makers have a framework to formally establish an audit objective. A baseline audit objective should be to determine compliance with requirements for access to CHRI for noncriminal justice purposes within the applicable jurisdiction of the audit program. Decision makers may also wish to consider incorporating additional business line functions, which could include training and customer service. Finally, in addition to audit objectives associated with assessments within the local user community, audit programs should also take into account the incorporation of internal assessments to ensure requirements are being met at the state and federal levels for administering access to local agencies.

Audit Scope

The scope of an audit identifies the boundaries from within which the objective will be accomplished. Audit scope defines the subject matter assessed and reported on, as well as the audit participants. Simply stated, audit scope answers questions regarding "what and who we audit."

General Audit Scope Considerations

The *CJIS Security Policy* sets the number of audit participants to all noncriminal justice agencies with access to CJI within the CSA's/SIB's jurisdiction. Audit programs should include a process to formally maintain a current list of all local agencies with access to criminal history records for noncriminal justice purposes. The list should include points of contact, information regarding the specific reasons, statutory authorities, and ORIs each agency leverages for access to criminal history records, as well as applicable organizational subcomponents with access. If outsourcing of administrative functions is occurring, then private and governmental contractors with access to criminal history records should also be identified. In addition, those agencies participating in programs such as VECHS should be identified. Audit programs may also take into account a tiered approach to categorize agencies. Primary agencies could be those with a more direct relationship with the state or federal agency. Secondary and subsequent levels of agencies could be subunits of primary agencies, receive information through primary agencies, or, based on risk, have infrequent or relatively low volumes of access. The categorization of agencies is also related to considerations for audit cycle and frequency which is discussed further in the methodology section.

At a minimum, it is recommended the scope of the audit program encompass the policies currently assessed during FBI CJIS Division audits of noncriminal justice access to criminal history records. Audit programs should also include within their scope other policy requirements applicable to the jurisdiction being considered. These may include requirements which are more restrictive in nature or applicable to access to other information sources such as state-only criminal history records.

Audit Methodology

Audit methodology is defined as the specific techniques and procedures used for gathering and analyzing information in order to assess performance. Audit methodology describes how the audit objective and scope will be accomplished and answers questions regarding "how we audit." The following sections present a discussion of methodology from the perspective of three primary phases based on chronological execution: pre-audit, assessment, and post-audit.

General Audit Methodology Considerations

Personnel and fiscal resources play a critical role in determining audit methodology. Constraints in these areas directly impact and may limit the options available to audit programs. Conversely, development of robust audit methodologies may serve as initial justification for managers to request additional resources. A thorough analysis of organizational priorities as well as the risks and benefits of particular options should be one of the first steps in the development of audit methodology. Options range from the establishment of offices or departments within the organization solely dedicated to performing audit functions to the outsourcing of audit functions to the private sector.

The number of audit participants and frequency of audits also play a primary role in determining the methodologies employed. The needs of a particular audit program may vary greatly depending on these variables. For a fixed number of audit participants and a fixed audit technique, audit frequency is inversely proportional to the resources available. For a fixed number of resources available and a fixed audit technique, audit frequency is directly proportional to the number of audit participants. The *CJIS Security Policy* sets the number of audit participants to all noncriminal justice agencies with access to CJI within the CSA's/SIB's jurisdiction. However, the *CJIS Security Policy* does not specifically dictate frequency. Audit programs should include a reasonable cycle for the conduct of noncriminal justice audits. While flexibility exists for planning purposes, as a best business practice, audit programs could incorporate a three-year audit cycle coinciding with the requirement to conduct audits of agencies with direct access. A triennial audit cycle also coincides with the *Security and Management Control Outsourcing Standard for Non-Channelers* requirement to audit a sample of authorized recipients and contractors. Consideration could also be given to using various combinations of audit techniques and frequency based on risk analysis and the categorization of agencies and their subunits in order to establish a good balance between the total number of audit participants, the resources available to execute audits, and the frequency by which audits occur.

Pre-Audit

Pre-audit activities provide a broad-based appraisal of the audit participant, as well as those activities necessary to coordinate the logistics of the audit. Pre-audit tasks should be centered on the initial gathering of information required for successful execution of the audit. Primary pre-audit tasks may include:

- Conducting internal research, which could include reviewing fingerprint submissions and III transactions as well as applicable statutes used by the audit participant to access criminal history.

- Contacting the audit participant to schedule the audit, explain the audit process, and request documentation. This could include advising the agency how to prepare for the audit and requesting copies of SOPs and organizational/system diagrams.
- Selection of organizational subcomponents/offices for review.
- Preparing surveys and requests for information and forwarding to the audit participant for completion. This could include data quality surveys of fingerprint submissions and high-level questions about agency processes.
- Reviewing documentation and information received from the audit participant.

Gaining an initial understanding of how criminal history records are accessed within an organization is of primary importance in developing an audit plan. The pre-audit phase may involve identification and selection of key nodes within an audit participant's organizational structure where assessments will be made. For example, a Department of Education within a state may consist of county boards and individual schools with access to criminal history records for background checks of teachers and other employees. Another example is a state-level Department of Children and Families consisting of multiple field offices throughout the state that receive criminal history records to adjudicate foster care applicants. Audit programs should include pre-audit procedures for selecting organizational subcomponents for review during the audit. These procedures should include factors used to prioritize selection. At a minimum, the following factors should be considered:

- Types of access to criminal history record information and relative volume of activity over a period of time.
- Use of multiple statutory authorities and the number of applicant types.
- Leveraging of programs which authorize dissemination to non-governmental entities and the re-use of criminal history records.
- Compliance issues identified during past audits.
- Use of name-based III access.
- Number of times audits have been conducted in the past.
- Use of contractors for administrative functions.
- Type and scale of systems used for distribution and storage of criminal history (electronic and hard copy).

Assessment

Within the context of this guide, assessments can generally be considered a comparison between policy requirements and an entity's processes associated with those policy requirements in order to determine compliance. The keys to this comparison are: (1) understanding the policy requirements and associated evaluation criteria; (2) obtaining relevant and sufficient information to understand an audit participant's operating practices; and (3) developing useful and logical conclusions based on professional judgment. There are a number of techniques or combinations of techniques for consideration as options for obtaining information about an audit participant's operating procedures and ability to comply with policy requirements associated with access to criminal history records:

- Interviews with audit participant personnel to include in-person and/or teleconferences.
- Surveys and questionnaires completed by the audit participant to include fingerprint and/or name-based III transaction surveys.

- Review of policy and procedural documents to include SOPs, statutes, administrative rules, and applicant forms.
- Review of case files and/or other documentation associated with individual transactions to include completed applications and personnel/licensing files.
- Demonstrations of information technology platforms to include on-line processes and internal databases.
- Physical inspection of work and storage areas to include on-site and off-site locations for hard copy and digital media.

The pros and cons of individual methods used to obtain information revolve around a hierarchy of perceived reliability. Direct observation and interviews made during an on-site visit are generally considered preferable to information gathered using more remote means such as mail-in or web-based questionnaires. However, there may be circumstances, based on resource availability and the relative risks associated with non-compliance, where more remote techniques could be considered more acceptable. While the application of audit methodology should remain relatively constant in order to ensure consistent assessment across the full spectrum of audit participants, audit methodology may vary for individual agency types and policies. Some policies may better lend themselves to on-site and more in depth assessments, while others may be adequately assessed more remotely. Audit programs should also incorporate flexibility in order to account for any unique circumstances that may warrant adjustments to methodology for a particular audit participant.

Audit criteria should be created in order to establish benchmarks against which performance is assessed. For each policy, criteria should primarily center on ensuring the audit participant has adequate processes, procedures and controls in place to meet policy requirements. In order to account for the myriad of unique processes, procedures, and controls employed across the full spectrum of audit participants, criteria should be established broadly enough to be applied consistently. In addition to criteria associated with process reviews, it is also important to consider the review of transactions in order to validate the audit participant's processes, procedures, and controls. However, caution should be exercised in cases where relatively small samples of transactions are reviewed in order to prevent making a final assessment based solely on information not necessarily representative of the audit participant's overall performance.

Reviews of transactions can be a particularly valuable tool used to validate an audit participant's processes, procedures, and controls. A sampling of individual transactions originating from an agency, such as fingerprint submissions or name-based III queries, can be selected for review. The sample could be derived from a random sampling formula or a screening of transactions to identify areas of interest. A survey can then be prepared using the individual transactions to request an audit participant provide specific information regarding the transactions related to compliance. For example, a survey of fingerprint transactions containing the names of subjects, dates of submission, transaction numbers, and other relevant data fields can be used to ask an audit participant to provide specific information regarding the reasons for the transactions and applicable statutory authorities. The completed survey can then be used to assist in the assessment of appropriate access to and use of criminal history records. The audit participant can also be asked to provide supporting documentation such as completed applications located in personnel case files or information systems.

The general premise for the formulation of questions to ask an audit participant is to establish how the audit participant ensures compliance with particular requirements through an explanation of the agency's processes, procedures, and controls. It is imperative the appropriate audit participant personnel are identified in order to obtain the most relevant information. In addition to specific questions associated with policy requirements, general questions should be formulated regarding the audit participant's organizational structure, mission, and operating systems. Audit participants should also be asked to describe the lifecycle of access to criminal history records. This would include a high-level chronological description of application and fingerprint submission, receipt and distribution of criminal history, adjudication, and maintenance activities. This will establish a framework for understanding the answers to more specific questions.

Post-Audit

Post audit activities are centered on reporting the results of assessments as well as reconciliation of compliance issues in order to formally complete the audit. The assessment phase of an audit transitions to the post-audit phase with the formulation of findings and recommendations. Post-audit should begin with closing out any open action items identified during the assessment phase in order to ensure final assessment decisions can be made. Coordination may also be required with applicable internal entities or departments such as subject matter experts located in program offices as well as legal staff in order to obtain any relevant information regarding system operation or policy interpretation.

In the formulation of findings and recommendations, auditors should determine whether or not sufficient information has been obtained to persuade a knowledgeable person that the findings are reasonable. This determination is made through a combination of professional judgment and subject matter expertise in the requirements being assessed. Facts and assumptions should be clearly identified and taken into account. Findings should be supported by information of sufficient quality (relevance, validity, reliability) and quantity (volume). It should be noted an increase in the volume of information does not necessarily equal or compensate for a lack of appropriateness or quality. This is particularly important when taking into account how findings and recommendations may impact audit participants to include allocation of fiscal, personnel, and other resources required to address compliance issues.

It is essential for methodology to include adequate mechanisms for reporting the results of the audit. There are a number of formats for consideration to include options such as letters, reports, verbal briefings, slide presentations, information packets, and posting results to websites. While more informal methods may be used, it is recommended a more formalized process be developed in order to properly document the results for reconciliation and historical reference purposes. In addition to formalized reporting procedures, it is also recommended audit participants are advised of the initial conclusions, potential compliance issues, and areas of concern prior to formal publication of the audit results. Regardless of the mechanisms or formats employed, audit reports should make the results clear and understandable. As a recommended starting point for development purposes, audit reports should address:

- Audit objective, scope, and methodology in sufficient detail for the audit participant to understand the context and perspective of the audit.

- Findings of compliance status relative to policy requirements. This could include varying degrees of compliance such as: in compliance, out of compliance, area of concern, and note of interest. Areas of concern and notes of interest could be used to highlight situations which may not warrant citation as a direct violation requiring a formal recommendation, but may increase the risk of a violation occurring or warrant documenting.
- Analysis describing why the conclusion regarding compliance status was made. The minimum elements of analysis associated with audit findings include condition, cause, and effect. Condition describes the existing situation (process, procedure, control). Cause explains the reasons or factors leading to the difference between the condition and the criteria, and is a critical element for development of recommendations. Effect establishes the impact or consequences of the difference between the condition and the criteria, and demonstrates the need for corrective action.
- Recommended actions to be taken by the audit participant to correct problems or improve performance.
- Request for follow-up actions to include formally responding to audit findings and recommendations.

As part of the reporting process, draft results should be presented to the audit participant for review and comment. This allows the audit participant the opportunity to provide operational clarifications and proposed edits, as well as the opportunity to provide a formal response describing corrective actions relative to the audit findings and recommendations. Audit programs could incorporate a response template to assist audit participants in addressing all findings and recommendations. Responses received from an audit participant should then be incorporated as part of the published final audit results.

Final audit results should be forwarded to appropriate offices responsible for determining if sufficient corrective actions have been taken by the audit participant to achieve compliance. Procedures should include review of corrective actions and follow-up as required to ensure the risk of future non-compliance has been sufficiently mitigated. The follow-up process should also establish sanctions or penalties for the failure to achieve compliance with policy requirements and include procedures for an audit participant to dispute audit findings and associated follow-up activities.

Prior to formally closing the audit, procedures should be in place to maintain relevant documentation associated with the audit. At a minimum, it is recommended audit programs have a process in place to retain final audit reports, agency responses, documents directly supporting compliance issues, and other information pertaining to general operating practices of the audit participant. The retention of these types of documents and information is particularly useful as a historical reference when planning future reviews of audit participants.

Additional Audit Considerations

Auditor Qualifications and Training

Audit staff should possess the knowledge, skills, and experience appropriate to execute the audit scope and objective. It is recommended auditors receive training as required to gain an appropriate level of expertise and comfort regarding the policy requirements associated with access to criminal history for noncriminal justice purposes. In addition, audit staff should be made aware of updates to existing policy requirements as well as changes to interpretations of those requirements. At a minimum, audit programs should incorporate resource materials and training made available by the Compact Council and FBI CJIS Division. Participation in formalized audit training programs offered in the private and governmental sectors may also warrant consideration.

Continuous Evaluation

Consideration should be given to establishing a process to continuously evaluate compliance with policy requirements across the entire jurisdiction of the audit program. As formal audits are only snapshots in time with respect to compliance, continuous evaluation processes can be quite effective in mitigating potential risks between audit cycles, especially if the frequency of formal audits is relatively low. Continuous evaluation techniques are also effective for gauging the long-term effectiveness of corrective actions implemented by audit participants. Continuous evaluation processes may also be beneficial in identifying triggers for off-cycle audits as well as in analyzing trends used to adjust audit methodologies. For example, automated or manual reports could be developed for civil fingerprint submissions and name-based III inquiries in order to identify anomalies or potential areas of concern by reviewing and comparing key data fields such as ORI, Reason Fingerprinted Field, Attention Field, Purpose Code, and Type of Transaction. Anomalies and potential areas of concern could then be isolated, and specific agencies contacted in order to supply necessary information required to gauge compliance with requirements.

Long-Term Strategies

It is imperative for audit programs to incorporate processes to continuously review, evaluate, update, and refine the audit objective, scope, and methodology. This is especially important when considering resource constraints and recent trends toward an ever-increasing number of authorized uses and users of criminal history records for noncriminal justice purposes. A more comprehensive application of trend and risk analysis may be required to strike the best balance between audit obligations and the resources available to execute a reasonably effective audit program. Audit programs should incorporate specific tools and products through the use of automation and software to collectively track audit results for historical comparison and trend analysis. Such tools and products will assist decision makers in making more informed decisions regarding the frequency and format of audits.

Acronyms

CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CSA	CJIS Systems Agency
III	Interstate Identification Index
ORI	Originating Agency Identifier
SIB	State Identification Bureau
SOP	Standard Operating Procedure
U.S.C.	United States Code
VECHS	Volunteer and Employee Criminal History System