ILLINOIS STATE POLICE DIRECTIVE
ADM-002, OFFICE OF INSPECTION AND AUDITS

RESCINDS:	**REVISED:**
ADM-002, 2022-003, revised 02-01-2022	11-20-2025 **2025-033**
RELATED DOCUMENTS:	**RELATED CALEA STANDARDS (6th Edition):**
ADM-140, ROC-002, PER-030, SRV-228	53.1.1, 53.2.1, 84.1.6

I. POLICY

The Illinois State Police (ISP) will maintain an Office of Inspection and Audits (OIA) for the purpose of conducting audits and reviews to:

I.A. Ensure objective appraisal or evaluation of department facilities, property, equipment, personnel, information technology (IT), information systems, receipts, expenditures, procurement, purchasing, administration, and operations.

I.B. Assist all members of management in the effective discharge of their responsibilities by furnishing them with analyses, appraisals, recommendations, and pertinent information.

I.C. Review the design of major new electronic data processing systems or major modifications of an existing system (ISP system) before their installation to ensure and advise that the system provides adequate audit trails and accountability.

I.D. Provide the services listed in I.A. and I.B. of this directive to other law enforcement agencies per the authority and at the direction of the Director.

II. AUTHORITY

30 ILCS 10/1001, et seq., the "Fiscal Control and Internal Auditing Act" (FCIAA)

III. DEFINITIONS

III.A. Audit – the practices and processes that provide the Director and other levels of management with the tools necessary to ensure compliance, economy, efficiency, and effectiveness of the agency's operation. In addition, an audit provides an objective evaluation of the Department's facilities, property, equipment, personnel, administrative activities, information systems, IT controls, and/or operational activities to ensure compliance with relevant laws, regulations, directives, and procedures.

III.A.1. Compliance Audit – determines whether administrators and/or programs are adhering to laws, rules, and directives.

III.A.2. Financial Audit – determines whether financial operations are properly conducted based on whether financial reports of an audited entity have complied with applicable laws and regulations.

III.A.3. Operational or Performance Audit – determines whether the entity is managing or utilizing its resources in an economical and efficient manner and the causes of any inefficiencies or uneconomical practices, including inadequacies in management information systems, administrative procedures, or organizational structures.

III.A.4. Pre-Implementation Review – determines whether an OIA-assessed major new ISP system, major ISP system modification, or non-major ISP system of significance to ISP operations provides for adequate audit trails and accountability, including proper internal controls built into the system before their installation.

NOTE: Pre-installation is the term used in the FCIAA (30 ILCS 10/2003(a)(3); however, Pre-Implementation Review is the current industry term.

III.A.5. Program Audit – determines whether desired results or benefits are being achieved, objectives established by the legislature or other authorizing body are being met, and the agency has considered alternatives that might yield desired results at a lower cost.

III.B. Chief Internal Auditor – a Certified Internal Auditor (by examination), a Certified Public Accountant with four years of internal audit experience, or an internal auditor with five years of experience named by the Director to oversee the ISP Internal Audit Function.

III.C. Compensating Control – a control that limits the severity of a finding and prevents it from rising to the level of a significant deficiency or a material weakness. Although a compensating control mitigates the effects of a control deficiency, it does not eliminate the control deficiency.

III.D. Control Deficiency – when an internal control does not facilitate management or employees, in the normal course of their duties, to prevent or detect errors, omissions, or other non-compliance on a timely basis.

III.E. Division Audit Liaison (DAL) – an individual, code or sworn, selected by their respective Division Deputy Director who will act as the Division's point of contact on all audit-related matters.

III.F. Exception – an identified deviation from a directive, statute, regulation, agreement, generally accepted IT control (e.g., National Institute of Standards and Technology (NIST)), Criminal Justice Information System (CJIS) policy, or another generally accepted standard or guideline.

III.G. Finding

III.G.1. Immaterial – a finding of enough significance that management awareness and corrective measures are necessary, but overall will not likely result in a material weakness.

III.G.2. Material – a finding whose significance is considered highly important to the area being audited.

III.H. Follow-up audit – an announced audit conducted by staff from the OIA, per the authority and direction of the Director, to review and evaluate those items that were identified during a previous audit as requiring attention or corrective action.

III.I. Information Technology (IT) Project Risk Assessment – an analysis conducted by OIA staff of the IT Project Risk Assessment Scoring Form submission to determine whether an approved IT Project development meets the definition of a major new ISP system or a major modification to an existing ISP system, or non-major ISP system of significance to ISP operations for a Pre-Implementation Review.

III.J. IT Project Risk Assessment Scoring Form, ISP 1-065 – the form completed and submitted for all IT Projects to the OIA by the Division Deputy Director/Office of the Director (OOD) Office Chief, or their designee, completed in coordination with the IT Project business or process owner or the Department of Innovation and Technology (DoIT) Chief Information Officer (CIO), or designee, for the OIA to complete a risk assessment, required documentation, select an audit review outcome and notify Command/management of OIA involvement in the IT Project.

III.K. Internal Audit Function – a process undertaken by a professional group of ISP personnel responsible for providing an organization with assurance and advisory services.

III.L. Material Weakness – a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the subject matter will not be prevented or detected.

III.M. Observation – a topic of interest for management that does not rise to the level of a finding.

III.N. Pre-Implementation Review Notification (as required by FCIAA) – a notification letter or report issued to Command/management prior to movement of the IT Project to production, outlining any control deficiencies or project risks identified in the OIA IT Project Pre-Implementation Review.

III.O. Project Charter – a DoIT document, available in the ISP Document Library, outlining the project purpose, high-level project description, cost estimate, key deliverables and their timeline, high-level requirements, and key stakeholders, their agency, and their role.

III.P. Quarterly Internal Audit Finding Follow-up report – an update provided every three months by the relevant division to the Chief Internal Auditor, or their designee, reporting the implementation status of corrective actions to remedy deficiencies identified by an audit.

III.Q. Significant Deficiency – a deficiency in internal control, or combination of deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process or report data reliably in accordance with the applicable criteria or framework such that there is more than a remote likelihood that a misstatement of the subject matter that is more than inconsequential will not be prevented or detected.

III.R. Special audit – an announced or unannounced audit of ISP or other law enforcement agency, conducted by the staff from the OIA per the authority and at the direction of the Director, to review and evaluate administrative and/or operational matters specifically identified by or requested by the Director.

III.S. State Internal Audit Advisory Board (SIAAB) – an oversight board created within FCIAA responsible for:

III.S.1. Promulgating a uniform set of professional standards and a code of ethics, based on the standards and ethics of the Institute of Internal Auditors (IIA), the U.S. Government Accountability Office, (i.e., generally accepted auditing standards and other professional standards as applicable) to which all State internal auditors must adhere;

III.S.2. Serving as a clearinghouse for the correlation of internal audit training needs and training designed to meet those needs; and

III.S.3. Coordinating peer review activities among the State's internal audit units.

III.T. Two-year audit plan – an annually updated plan of audits for the subsequent two-years as required by FCIAA. This plan is developed with input from the OIA staff, ISP Command/management, reviews of external audits, and questionnaires to assess risk.

IV. RESPONSIBILITIES

IV.A. OIA personnel will perform audits as part of an on-going, annually-revised two-year risk-based audit plan which will include periodic review of all agency operations, information systems, prior internal audit reports, post audit reports, observations, and requests by the Director.

IV.B. The Deputy Director of each division is responsible for appointing a DAL for their respective division. Upon a change of the DAL, the newly appointed DAL will notify the Chief Internal Auditor of the change.

IV.C. The Deputy Director/OOD Chief, or designee, is responsible for completing and submitting via email to the ISP.InspectionandAuditsInbox, an IT Project Risk Assessment Scoring Form, ISP 1-065, including completion of the system narrative therein. The form should be completed in coordination with the Division/OOD Office IT Project business or process owner and the ISP DoIT CIO, or designee, for the OIA to complete a system risk assessment via availability and review, at a minimum, of the IT Project Charter, business requirements, technical requirements, and, if applicable, vendor contract and statement of work, record required documentation, select an audit review outcome, and notify Command/management of the OIA's necessary involvement in the IT Project.

IV.D. Employees will give full cooperation to personnel conducting audits and reviews to include, but not be limited to, making all files or records (e.g., program, fiscal, administrative, personnel, investigative, IT Project, Division of Internal Investigation (DII), confidential source, and juvenile), property, and equipment available for review/examination upon reasonable request.

V. PROCEDURES

V.A. Interview Requests

An employee who wishes to be interviewed in conjunction with an audit may make this request known:

V.A.1. Through the chain-of-command

V.A.2. By directly contacting their respective Deputy Director's Office

V.A.3. By directly contacting staff from the OIA

V.B. Management Assistance

V.B.1. The OIA will assist all members of management in the effective discharge of their responsibilities by furnishing them with analyses, appraisals, recommendations, and pertinent comments concerning the activities reviewed.

V.B.2. OIA auditors are concerned with any phase of department activity when they can be of service to management. This goes beyond the accounting and financial records to obtain a full understanding of the operations under review. The attainment of this overall objective of service to management involves such activities as:

V.B.2.a. Determining the adequacy of financial records and performance reports that disclose the present condition and the results of past operations of an organization or program.

V.B.2.b. Reviewing the extent to which assets are accounted for and safeguarded from losses of all kinds.

V.B.2.c. Ascertaining compliance and degree of adherence to prescribed rules, policies, programs, and mandates.

V.B.2.d. Evaluating the efficiency, effectiveness, and economy of programs and operations.

V.B.2.e. Conducting a Pre-Implementation Review of an ISP system to determine the system provides for adequate audit trails and accountability, including proper internal controls built into the system before their installation.

V.B.2.f. Reviewing the adequacy, accountability, and reliability of information systems and IT controls.

V.B.2.g. Ensuring prescribed uniformity of procedures as appropriate throughout the Department, particularly those concerning administration, operation, supervision, personnel, and department standards of excellence, fairness, and safety of officers and employees.

V.B.3. OIA staff members are prohibited by internal audit standards from providing or advising of specific solutions to correct identified problem areas. Advisory services by OIA staff can provide advice to ISP personnel on the design and implementation of new policies, processes, systems, and services; provide training; and facilitate discussions about risks and controls without taking on management responsibilities in order to maintain OIA staff independence and objectivity in the ISP activities audited.

V.C. Conducting Audits

V.C.1. The Chief Internal Auditor will send notification to the appropriate Command/management describing the proposed type and scope of the audit or Pre-Implementation Review and requesting the entity being audited to attend an entrance conference.

V.C.2. The entrance conference will be held on the starting date of the audit between OIA staff and the desired personnel of the audited entity.

V.C.2.a. The purpose, scope, anticipated timeframe of the audit, procedures to be followed, and reporting practices will be discussed at this meeting.

V.C.2.b. Upon initiation of a Pre-Implementation Review, the Deputy Director/OOD Office Chief, or designee, will notify the OIA in writing of the anticipated system go-live date and any changes to the system go-live date. These notifications should be sent to the ISP.InspectionandAuditsInbox.

V.C.2.c. Emphasis is placed on the practice of reviewing exceptions, and/or recommendations and findings, during the course of the audit prior to the issuance of a final report.

V.C.3. OIA staff will perform audit fieldwork.

V.C.4. At the conclusion of fieldwork, a draft report or Pre-Implementation Review Notification will be prepared, as applicable. The draft report will include any findings and observations resulting from the exceptions/control deficiencies identified during fieldwork.

V.C.5. The draft report will be issued to the audited entity and Command/management of the area audited. The audited entity will be afforded the opportunity to request an exit conference.

V.C.5.a. If an exit conference is not requested, the audited entity will provide written responses to the findings within the time designated by the OIA. The audited entity's response options are:

V.C.5.a.1) "Concur" – the Division audited agrees with the finding.
V.C.5.a.2) "Do not concur" – the Division does not agree with the finding.

V.C.5.b. The response will also include a corrective action plan and an estimated completion date of the corrective action. If corrective action is impeded by fiscal or staffing issues outside of ISP control, the use of compensating controls should be considered until appropriate resources are allocated.

V.C.5.c. If an exit conference is requested, OIA staff will meet with the appropriate Command/management to discuss the report and potential findings. Once OIA staff and the audited entity agree on the findings, the audited entity will then provide a written response for each finding following the procedures located in V.C.5.a. through V.C.5.b. above.

V.C.6. Upon receipt, the OIA will prepare a final report to include the responses provided by the audited entity. The OIA will forward this report to the Director, audited entity Command/management, and the OOD COS.

V.D. Follow-up

V.D.1. Provided with the final report will be a Quarterly Internal Follow-Up Review form. This form is used by the OIA as a tool to monitor the implementation progress of the corrective action cited in the recommendations and the audited entity's initial response to the audit findings.

V.D.2. Quarterly, on or before the date noted on the form, the Division will complete and forward the follow-up form to the OIA.

V.D.3. The following response formats must be used when completing the quarterly follow-up form:

V.D.3.a. "Fully Implemented" – the Division accepted the recommendation and completely implemented the corrective action to a finding.

V.D.3.a.1) The Division must provide a statement of the corrective action taken.
V.D.3.a.2) The Division must also submit examples proving implementation with the follow-up form. An example proving implementation must be provided for each exception contributing to the finding.

V.D.3.b. "Partially Implemented" – the Division accepted the recommendation and partially implemented the corrective action to a finding.

V.D.3.b.1) The response must include a statement of what corrective action the Division took and include an example for proof of partial implementation.

V.D.3.b.2) The response must also include a clear reason why the Division did not implement part of the corrective action, the corrective action the Division will take, and an estimated date of completion.

V.D.3.c. "Not implemented" – the Division accepted the recommendation but did not implement the corrective action to a finding. The response must include a clear reason why the Division did not implement the corrective action, the corrective action the Division will take, and an estimated date of completion.

NOTE: All false documentation and information reported is subject to disciplinary action as outlined in ISP Directive ROC-002, "Rules of Conduct," ISP Directive PER-030, "Complaint and Disciplinary Investigations," and applicable collective bargaining agreements.

V.D.4. Final determination of the corrective action's implementation status will be made by the Chief Internal Auditor.

V.D.4.a. Appeals of the final determination will be forwarded, in writing, to the OOD Chief of Staff (COS).

V.D.4.b. The COS will assist the First Deputy Director (FDD) in mediating the dispute.

V.D.5. The follow-up process will continue until all finding corrective actions have achieved a fully implemented status or any remaining corrective action exceeds the Division's authority to implement.

V.D.5.a. The responsibility for continued follow-up/corrective action will be transferred to the Division with the authority to implement such action.

V.D.5.b. No further follow-up/corrective action will be required when such action exceeds the authority of any ISP Division to implement.

NOTE: The Chief Internal Auditor will make the final determination if follow-up action should be transferred or terminated by an ISP Division as described in V.D.5.a. and V.D.5.b. above.

V.D.6. A follow-up audit may be performed to ensure that actions reported by the audited entity are effective and functioning as intended.

V.D.7. Each Division/OOD Office will provide a report regarding any finding with corrective action that has not been fully implemented after one year. This report will be compiled and presented to the Director's office for review as outlined in ISP Directive ADM-140, "Administrative Reporting."

V.E. FCIAA Internal Control Certification (ICC) Facilitation/Advisor

V.E.1. The Director has designated the OIA as the facilitator of the annual FCIAA Internal Control Certification required by FCIAA Section 3003.

V.E.2. Each Division/OOD Office will participate in an annual evaluation of internal controls to facilitate the Director's certification to the Auditor General by May 1 each year.

V.E.3. Each Division/OOD Bureau will complete an ISP FCIAA Internal Control Certification Checklist, ISP-1067, adopted by ISP based on the guidelines established by the Comptroller's Office in coordination with the Illinois Department of Central Management Services (CMS) and approved by the Legislative Audit Commission (LAC) pursuant to FCIAA Article 3 Section 3002.

V.E.4. Each Division/OOD Office will submit via email to the ISP.InspectionandAuditsInbox, the completed checklist, an ISP FCIAA Internal Control Certification CAP, form ISP 1-066, if applicable, and a certification letter to the Director that:

V.E.4.a. The systems of internal fiscal and administrative controls of the State agency fully comply with the requirements of FCIAA Article 3 Section 3001; or

V.E.4.b. The systems of internal fiscal and administrative controls of the State agency do not fully comply with the requirements of FCIAA Article Section 3001.

If the systems do not fully comply with the requirements of FCIAA Article 3 Section 3001, or the Division/OOD Office has reported material weakness in the external compliance examination, the process owner must complete and submit an ISP FCIAA Internal Control Certification CAP, form ISP 1-066, to describe each weakness in the systems of internal fiscal and administrative controls, the materiality of the weakness, and the plans and schedule for correcting the weakness, or a statement of the reasons why the weakness cannot be corrected.

V.F. Outside Agency Requests

V.F.1. At the discretion of the Director, the ISP may conduct an audit of an outside law enforcement unit.

V.F.2. All reports, documents, and work papers used during the audit of the outside law enforcement unit are property of the ISP and will be released, or held confidential, as required by law.

Indicates new or revised items.

-End of Directive-