

UNIVERSITY OF ILLINOIS SYSTEM

Audit Policy Manual

Office of University Audits

AUDIT POLICY MANUAL

TABLE OF CONTENTS

Page

POLICY

- Internal Audit Charter 1
- Mission/Vision Statement 2
- State of Illinois Fiscal Control and Internal Auditing Act 3
- Confidentiality 4
- Independence and Objectivity 6
- Quality Assurance 7

AUDIT PLANNING

- Annual Audit Planning 8

AUDIT PROCESS

- Overview 10
- Risk Assessment Process 12
- Opening Conference 13
- Fieldwork 14
- Audit Observations 15
- Workpapers 16

REPORTING AND FOLLOW-UP

- Reporting 18
- Follow-up 20
- Annual Report 22

PERSONNEL

- Performance Appraisal Process 23
- Training and Professional Development 24

ADMINISTRATIVE PROCEDURES

- Computers 26
- Auditor Timekeeping 27
- Records Retention Policies 28
- General Policies 29
- Dress Code 30

POLICY

INTERNAL AUDIT CHARTER

See https://www.audits.uillinois.edu/internal_audit_charter

POLICY

MISSION STATEMENT

The mission of the Office of University Audits (OUA) is to provide independent and objective assurance, consulting/advisory, and investigation services to protect and strengthen the University of Illinois System (U of I System) and its related organizations.

VISION STATEMENT

Be an innovative driver of positive change.

GUIDING VALUES

We perform all that we do with:

- Objectivity
- Independence
- Integrity
- Excellence
- Innovation
- Professionalism

STRATEGIC GOALS

1. The OUA will continue to cultivate relationships and understanding through communication with the Board of Trustees (board) and senior leadership of the U of I System.
2. Serve as counsel to the board, the Audit, Budget, Finance and Facilities Committee of the board (ABFFC), management, and other constituents.
3. Enhance audit effectiveness and efficiencies.
4. Provide a professional, well-trained, and motivated team in the delivery of internal audit services.
5. Perform audit activities by utilizing a dynamic comprehensive audit process and plan based on assessed risk, in compliance with the Institute for Internal Auditing's 2024 Global Internal Audit Standards (GIAS).

POLICY

STATE OF ILLINOIS
FISCAL CONTROL AND INTERNAL AUDITING ACT

The Fiscal Control and Internal Auditing Act (Illinois Compiled Statutes, 30 ILCS 10/1001) (FCIAA) is the state legislation which designates the chief executive officer of every state agency as responsible for establishing and maintaining an effective system of internal control and provides guidance and mandates for internal audit activities of state agencies.

The State Internal Audit Advisory Board (SIAAB), as established by FCIAA, is responsible for promulgating a uniform set of professional standards and a code of ethics to which all state internal auditors must adhere, supporting and supplementing the training needs of the state's internal auditors, and establishing standards for the conduct of external and internal quality assurance assessments. These requirements are included in the SIABB's Bylaws. Excerpts from each section are included below.

Article II, Section III, Professional Auditing Standards, states that "All audits performed by the internal audit staffs of State agencies shall be conducted in accordance with Standards adopted by SIAAB as provided by FCIAA. These Standards shall be summarized in the Quality Assurance Matrix on SIAAB's website and shall include...The 2024 Global Internal Audit Standards (GIAS) published by the Institute of Internal Auditors (IIA)....."Article II, Section IV, Code of Ethics, states that "All State auditors shall adhere to…standards of conduct which were derived from the IIA's 2024 Global Internal Auditing Standards, Domain II: Ethics and Professionalism."

Article II, Section V, addresses continuing professional education (CPE), and the qualifying and recording of CPE activities.

POLICY

CONFIDENTIALITY

DEFINITION

Confidential information is information of a proprietary or sensitive nature about the U of I System, its students, contracted agents, and employees.

POLICY

Internal auditors respect the value and ownership of information they receive and do not discuss information without appropriate authority unless there is a legal or professional obligation to do so.

All audit staff are required to formally acknowledge their understanding of the confidentiality requirements. Confidential information acquired by audit staff through their employment must be held in strict confidence. Audit staff shall be prudent in the use and protection of information acquired in the course of their duties. It is to be used solely for U of I System purposes and must not be used as a basis for personal gain by the audit staff, or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the U of I System. Confidential information is transmitted only to those individuals who need the information to discharge their duties as U of I System employees or audit staff. Any other dissemination of workpaper or correspondence contents must be approved by the appropriate director. Any dissemination without authorization will be considered serious misconduct and could result in suspension or dismissal.

REPORT SECURITY AND CONTROL

Access to audit reports and management communications that include audit details is restricted to audit staff.

Illinois statute exempts certain audit information from being available for public inspection and copying.

ILLINOIS COMPILED STATUTES, CHAPTER 5, GENERAL PROVISIONS

140. ILLINOIS FREEDOM OF INFORMATION ACT

7. Exemptions from inspection and copying (effective July 1, 1984).

   (1). The following shall be exempt from inspection and copying:

   .
   .
   .

   (m) **Communications between a public body and an attorney or auditor representing the public body that would not be subject to discovery in litigation, and materials prepared or compiled by or for a public body in anticipation of a criminal, civil or administrative proceeding upon the request of an attorney advising the public body, and materials prepared or compiled with respect to internal audits of public bodies**. [Emphasis added]

Due to the sensitive and confidential nature of our audit reports, all efforts should be made to keep reports protected from public disclosure. Audit reports should not be voluntarily disclosed outside of the U of I System and should only be released at the express direction of the president or upon presentation of a valid court order.

All audit-related communications (e.g., emails, documents, etc.) should contain notification of the exemption.

To protect our exemption provided under the Freedom of Information Act (FOIA), University Audits will require authorized review of reports or workpapers by an outside party to be performed in our office, under our control as to access, review, and notes taken by the outside party. It is our policy to not permit the removal of documents, or copies thereof, from our office.

Some audits may be performed under the direction of university counsel as a matter of attorney-client privilege. Audits are performed this way solely for the purpose of assisting university counsel in providing their legal advice.

POLICY

INDEPENDENCE AND OBJECTIVITY

DEFINITIONS

Independence is defined, per GIAS, as “the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.”

Objectivity is defined, per GIAS, as “An unbiased mental attitude that allows internal auditors to make professional judgments, fulfill their responsibilities and achieve the Purpose of Internal Auditing without compromise. “

POLICY

Per GIAS 7.1 Organizational Independence, “The chief audit executive must confirm to the board the organizational independence of the internal audit function at least annually. This includes communicating incidents where independence may have been impaired and the actions or safeguards employed to address the impairment.”

The OUA’s organizational independence is demonstrated through the Internal Audit Charter; ABFFC Audit Function Charter, and the OUA organization chart. Per GIAS 2.1 Individual Objectivity, “Internal auditors must maintain professional objectivity when performing all aspects of internal audit services. Professional objectivity requires internal auditors to apply an impartial and unbiased mindset and make judgments based on balanced assessments of all relevant circumstances. Internal auditors must be aware of and manage potential biases.”

Annually, and as situations arise during the year, each auditor will disclose any potential conflicts or independence issues. To maintain independence and objectivity, staff members will not be assigned audits involving the following instances:

1. Any situation that involves a member of the auditor's immediate family, as defined by the U of I System Policy on Conflicts of Commitment and Interest
2. Any activity that the auditor previously performed or supervised, unless at least one year has elapsed.
3. Any other situation in which a conflict of interest or bias is present or may reasonably be inferred.

If an auditor works on an engagement where the perception of a conflict of interest could exist, an action plan to mitigate the perceived or actual conflict should be documented in the workpapers.

POLICY

QUALITY ASSURANCE

GENERAL

The establishment and implementation of a quality assurance and improvement program for the OUA is required by GIAS and includes both internal and external assessments. Per GIAS, "A quality assurance and improvement program is designed to evaluate and promote the internal audit function's conformance with GIAS, achievement of performance objectives, and pursuit of continuous improvement."

INTERNAL ASSESSMENTS

Internal assessments include both ongoing monitoring of the performance of the internal audit activity and periodic self-assessments. Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the internal audit activity, and is incorporated into the routine policies and practices used to manage the internal audit activity. Periodic self-assessments are conducted to evaluate conformance with GIAS on a more holistic basis.

The SIAAB Guidance #09 and the IIA Quality Assessment Manual offer various possible methods of conforming to the periodic self-assessment requirement.

The results of periodic self-assessments are communicated to the vice president-chief financial officer, president, and ABFFC upon completion, and the results of ongoing monitoring are communicated at least annually as required by GIAS.

EXTERNAL ASSESSMENTS

In compliance with GIAS and SIAAB Bylaws, an external assessment of the OUA will be performed every five years by a qualified, independent assessor or assessment team from outside the U of I System. The results of external assessments are communicated to the vice president-chief financial officer, president, and ABFFC upon completion.

AUDIT PLANNING

ANNUAL AUDIT PLANNING

OVERVIEW

Each year, a flexible two-year risk-based internal audit plan of U of I System audits is developed. The executive director of University Audits discusses the plan with senior management and submits to the ABFFC for feedback and concurrence. In accordance with FCIAA, the president approves the Audit Plan by June 30 of each fiscal year.

An annual risk assessment is performed to establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the U of I System's goals. Development of the plan considers the U of I System's Strategic Framework, risk management framework, OUA management's judgment of risks, legislatively required audits, and input from senior management and the ABFFC.

RISK CATEGORIES

Categories of risk we assess include, but are not limited to, the following:

- Financial risks deal with internal controls over and reporting of financial transactions, including assets, liabilities, revenues, and expenditures.
- Compliance risks deal with the adequacy of a unit's system of internal controls to ensure compliance with applicable laws, regulations, and policies.
- Operational risks deal with the unit's ability to use its resources in an effective and efficient way.
- Reputational risks deal with issues that may not be significant from a financial, compliance, or operational perspective, but could have a potentially negative public perception impact.
- Safety risks include events, situations, or other circumstances that have the potential to cause harm to individual(s), including students, employees, and the public.

FCIAA requires the two-year plan to include:

- Audits of major systems of internal accounting and administrative control such that each system is addressed every two years. The major systems are to be given consideration as part of the documented risk assessment process; the amount of coverage of each system is based on risk. Due to the U of I System's multi-faceted, decentralized structure, these audits are performed using a combination of the Illinois Comptroller Statewide Accounting Management System (SAMS) Manual's transaction cycle approach and organizational structure approach. Our audits can be either a broad system process or at a segmented unit level. We use the following major systems, as outlined via the SAMS Manual:
    - ☐ Organization and Management
    - ☐ Administrative Support Services
    - ☐ Budgeting, Accounting, and Reporting
    - ☐ Purchasing, Contracting, and Leasing
    - ☐ Expenditure Control
    - ☐ Personnel and Payroll
    - ☐ Property, Equipment, and Inventories
    - ☐ Revenues and Receivables
    - ☐ Cash and Local Funds
    - ☐ Grant/Research Administration
    - ☐ Information Technology

- Audit testing that includes:
    - ☐ The obligation, expenditure, receipt, and use of public funds of the state and of funds held in trust to determine whether these activities are in accordance with applicable laws and regulations.
    - ☐ Grants received or made to determine that the grants are monitored, administered, and accounted for in accordance with applicable laws and regulations.
- Review of the design of major new information technology systems and major modifications to existing systems before installation to determine whether the systems provide adequate audit trails and accountability.
- Special audits of operations, procedures, programs, information technology systems, and activities as directed by the president or board, as applicable.

AUDIT PROCESS

OVERVIEW

ENGAGEMENT TYPES

Assurance Audit
Assurance engagements are services through which the internal auditors perform objective assessments of an organization's governance, risk management, and control processes for the purpose of increasing stakeholders' confidence.

Investigation
Investigation engagements are a systematic process of gathering evidence, conducting interviews, and analyzing records to determine if alleged civil or criminal violations of state or federal laws, or violations of U of I System policies and procedures occurred. The result of such engagements may support prosecution or disciplinary action.

Consulting/Advisory
Consulting/advisory engagements are services through which internal auditors provide advice to an organization's stakeholders without providing assurances or taking on management responsibilities. The scope and procedures involved in consulting engagements are either directed by management or agreed upon with management. Reporting for consulting engagements is generally made directly to management requesting the service. Advisory services are less formal in nature and may include providing counsel, advice, facilitation, and training.

EXAMPLES OF AREAS OF FOCUS

Internal control focus considers whether the unit is conducting its financial and business processes under an adequate system of internal control, as required by the U of I System policy and guidelines and good business practice.

Compliance focus considers U of I System policies and procedures and external requirements. Examples of external requirements include donor intent, federal and state laws and regulations, National Collegiate Athletic Association legislation, and Big Ten Conference legislation.

Financial focus considers the accuracy of financial information of assets, liabilities, revenues, expenditures, or other financial presentations.

Information technology (IT) focus considers the internal control environment of automated information processing systems and how people use those systems which typically include system input, output, and processing controls; backup and recovery plans; system security; and computer facilities.

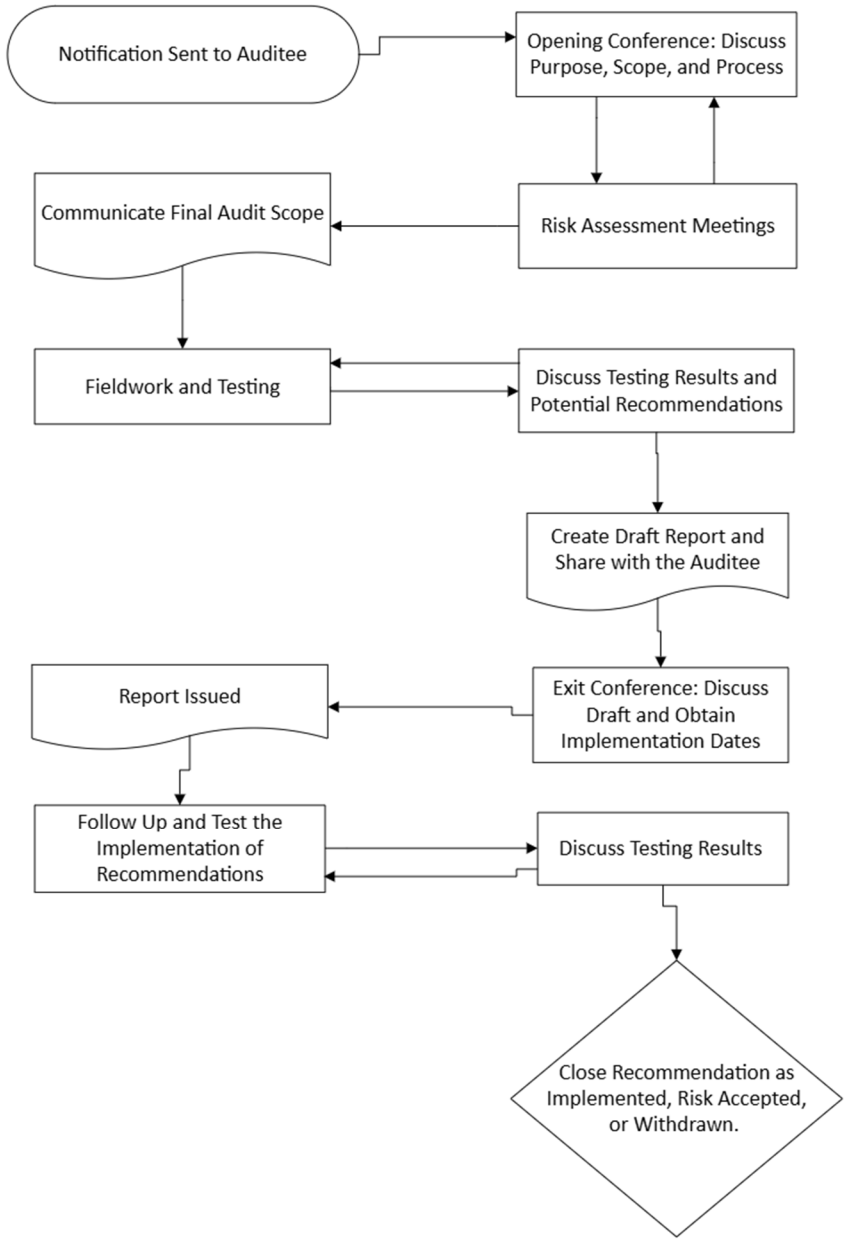
Operational focus considers the use of unit resources and whether those resources are being used in efficient and effective ways. An operational focus is typically combined with other focus areas such as internal control and compliance.

Data Analytics is a methodology that uses data to evaluate risk and related internal controls on a more frequent basis. It involves using various techniques to identify anomalies, patterns or trends, and other indicators, such as non-compliance with U of I System policies, which may reveal control weaknesses. It can be used to assess the risk of a particular business cycle or to perform detailed transaction analysis against cut-offs or thresholds. The analysis is typically U of I System-wide, with more detailed reviews of transactions occurring as needed based on the results. It is also used as an element of the annual risk assessment for audit plan development.

AUDIT PROCESS

OVERVIEW

.



AUDIT PROCESS

RISK ASSESSMENT PROCESS

The risk assessment process starts with the auditor's identification and analysis of risk for an audit based on the objective or reason that it was placed on the OUA's two-year annual audit plan.

According to GIAS, internal auditors must then develop an understanding of the activity under review to assess the relevant risks by gathering reliable, relevant, and sufficient information regarding:

- The organization's strategies, objectives, and risks relevant to the activity under review.
- The organization's risk tolerance.
- The governance, risk management, and control processes of the activity.
- Applicable frameworks, guidance, and other criteria that can be used to evaluate the effectiveness of these processes and whether objectives and goals have been met.

GIAS also state that as part of due professional care, internal auditors should consider input from management of the activity under review to gain insight into the business objectives, significant risks, and controls.

Internal auditors must review the information gathered and identify the risks to the engagement by:

- Identifying potentially significant risks.
- Considering specific risks related to fraud.
- Evaluating the significance of the risks and prioritizing them.

The process of risk assessment is not linear. It begins before the entrance conference and continues during and after the entrance conference until the objective and scope have been determined by the auditor, approved by the director (delegated by the executive director), and communicated to the auditee. Throughout the engagement, the auditor should constantly be aware of and evaluate any information that would change the risk assessment.

Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client. Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.

AUDIT PROCESS

OPENING CONFERENCE

The opening conference should be held to explain the audit process and gather any initial information.

The following will be reviewed during the opening conference:

- The entire audit process including how concerns will be handled.
- The preliminary objective(s) and scope of the audit.
- Identification of key personnel needed to answer detailed questions concerning the functions or processes within the unit.
- Potential problem or risk areas that the auditee would like to be considered for inclusion within the audit scope. The frequency the department head/director or activity owner wants to be updated on audit progress and findings.

Certain audits, such as investigative audits or assurance audits that focus on data analytics or compliance, may not have an opening conference.

AUDIT PROCESS

FIELDWORK

In accordance with GIAS, to implement the engagement work program, internal auditors gather information and perform analysis and evaluations to produce evidence. These steps enable the internal auditor to:

- Provide assurance and identify potential findings.
- Determine the root cause, effects, and significance of the findings.
- Develop recommendations and/or collaborate with management to develop action plans.
- Develop conclusions.

DEFINITION AND PURPOSE

Fieldwork is the process of gathering evidence and analyzing and evaluating that evidence.

Throughout fieldwork, professional judgment should be used to: a) determine whether evidence gathered is relevant, reliable, and sufficient to provide a reasonable basis upon which to formulate potential engagement findings and conclusions. and b) based on the information available, reassess the audit objectives, scope, and procedures to ensure efficient use of audit resources (e.g., should the remaining audit steps be eliminated, should the objective or scope be modified, have more efficient procedures been identified, or should additional hours be allocated to achieve an expanded audit objective). Discuss with audit management and communicate timely the impact of significant proposed changes, and document changes in audit objectives, scope, and procedures in the workpapers.

Fieldwork includes:

1. Gaining an understanding of the activity, system, or process under review and the prescribed policies and procedures, supplementing and continuing to build upon the information already obtained in the risk assessment process.
2. Observing conditions or operations.
3. Interviewing people.
4. Examining assets and records.
5. Analyzing data and information.
6. Identifying key control points in processes.
7. Determining if appropriate action has been taken regarding significant audit concerns and corrective actions reported in prior audits.
8. Conducting compliance testing.
9. Conducting substantive testing.
10. Evaluating and concluding on the adequacy (effectiveness and efficiency) of internal controls.
11. Discussing potential risks and recommendations with the auditee and the cost/benefit assessment that led to recommendations.

Any changes to the objective and scope that occur during fieldwork should be approved by the director (delegated by the executive director) and communicated to the auditee.

AUDIT PROCESS

AUDIT OBSERVATIONS

CRITICAL ASPECTS OF THE AUDIT OBSERVATION

FINDING – DESCRIPTION OF OBSERVATION [CONDITION]
This section of the observation should contain a clear and concise statement of the condition. GIAS states the condition is the difference between the evaluation criteria (e.g., policy) and the existing state. The statement should be concise but provide enough detail to support the reader's understanding of the problem.

DISCUSSION AND BACKGROUND – ANALYSIS OF THE AUDIT FINDING [CRITERIA]
Per GIAS, the criteria are the "specifications of the desired state of the activity under review."

The auditor should document the analysis of the problem which should include support for GIAS, policies, procedures, and/or good business practice, as well as support for the condition found.

An evaluation of the significance of the condition should also be included and results in the disposition and risk ranking decisions GIAS states that when determining the significance, internal auditors should consider:

- The impact and likelihood of the risk.
- The risk tolerance of the organization.
- Any additional factors important to the organization.

ROOT CAUSE – DIRECT REASON THE CONDITION EXISTS [CAUSE]
The auditor should identify probable root causes (as opposed to the symptoms) for the issue. Per GIAS, "identifying the root cause involves collaboration with management, who may be in a better position to understand the underlying causes for the difference."

RECOMMENDATION [EFFECT AND CORRECTIVE ACTION]
Per GIAS, Internal Auditors must determine whether to develop recommendations, request action plans from management, or collaborate with management to agree on actions to:

- Resolve the differences between the criteria and current state.
- Mitigate identified risks to an acceptable level.
- Address the root cause of the finding.
- Enhance or improve the activity under review.

The recommendation is the culmination of the information above along with the corrective action. The auditor should include the finding, a statement of risk which is sufficient to answer the "so what?" question, and the recommended corrective action.

RISK RANKING
The auditor should document their assessment of the risk level associated with the finding. GIAS states that "…the extent of the exposure is an estimate informed by the auditor's professional judgement with input from management of the activity under review." The risk ranking criteria were created in collaboration with senior U of I System leaders and the ABFFC.

DISCUSSION WITH AUDITEE
The auditor should document their discussions of the finding and recommendation with the auditee.

AUDIT PROCESS

WORKPAPERS

WORKPAPER PREPARATION

The workpapers are the connecting link between the audit assignment, the auditor's fieldwork, and the final report. Workpapers contain the records of the planning and risk assessment process, audit procedures, fieldwork, and other documents relating to the audit. The workpapers provide the basis for supporting our conclusions and engagement reports, as well as evaluating the OUA's quality assurance program to demonstrate the OUA's conformance with GIAS.

WORKPAPER REVIEW

Auditor

The auditor should conduct a review of the workpapers prior to submission to the appropriate member of audit management to determine whether they are relevant to the audit objectives, reliably evidence the audit work performed (i.e., factual and current), and sufficiently support the audit findings. Auditors should apply professional skepticism in review of all materials and ensure that OUA workpaper guidelines are followed. The auditor should review all comment forms to be certain that all issues have been resolved within the workpapers since the comment forms will not be retained. All other information obtained during the audit should be reviewed to determine whether all documentation relevant to the audit has been included in the audit workpapers. Documentation obtained and not relevant to the audit or no longer needed should be returned or destroyed upon completion of the audit, as applicable.

Audit Management

According to GIAS, a review of the engagement documentation by the engagement supervisor and the executive director is necessary to ensure it contains relevant, reliable, and sufficient information that enables a prudent, informed, and competent person to reach the same conclusions as those who conducted the engagement. Approval should be documented by the engagement supervisor at the time the risk assessment process is completed, audit procedures have been developed, and when completed workpapers are reviewed. While directors are delegated responsibility for engagement-level oversight and execution, the executive director retains ultimate accountability for engagement objectives, scope, work program adequacy, and results, consistent with GIAS.

Audit management will:

- Determine compliance with workpaper policies and procedures.
- Review the risk assessment process to ensure that objectives are defined.
- Review the audit procedures to ensure that they are adequate to accomplish the objectives.
- Review the referenced workpapers to ensure they support the procedures performed and all procedures have been completed.
- Determine that the workpapers adequately document the conclusions reached in the report.
- Confirm that all observation forms prepared have been discussed with the appropriate member of management, root cause has been identified, and the disposition of the audit concern is documented.

For assurance and investigative audits, audit management will perform three levels of review for the draft report as follows:

- The engagement director will review and approve the draft report.
- A peer director will review and provide any suggestions or feedback to the audit team.
- The executive director will review and approve the draft report.

For consulting engagements, audit management will perform two levels of review for the draft report as follows:

- The engagement director will review and approve the draft report.
- The executive director will review and approve the draft report.

All final reports are reviewed and approved by the engagement director and the executive director and are distributed by the executive director.

PERSONAL HEALTH INFORMATION (PHI) IN WORKPAPERS

The auditor should determine if PHI is necessary to evidence the audit work performed. If PHI is needed, U of I System policy over proper storage will be followed.

REPORTING AND FOLLOW-UP

REPORTING

DRAFTING THE REPORT

Per GIAS, the report is to include the "engagement's objectives, scope, recommendations and action plans if applicable, and conclusions." The final communication for assurance engagements also must include:

- The findings and their significance and prioritization.
- An explanation of scope limitations, if any.
- A conclusion regarding the effectiveness of the governance, risk management, and control processes of the activity reviewed.
- Individuals responsible for addressing the findings and the planned date by which the actions should be completed.
- Any actions already taken by management to address the findings.

Any observations that are significant to communicate to management or background information that would help readers with the context or risks should be included.

All parties are responsible for adhering to the established reporting format standards for assurance and investigative audits. Consulting reports are not standardized by their ad hoc nature, and as such their unique formats are to be agreed to by audit management and the auditee to meet the needs of the specific engagement.

EXIT CONFERENCE

An exit conference will generally be held for all assurance and consulting engagements. An exit conference for investigative engagements will depend on the nature of the work and whether recommendations were made. The purpose of an exit conference is to discuss with the auditee the content of the report. The exit conference provides the opportunity for the auditee to clarify specific items and to express views on the recommended action plans and other information presented in the draft report.

TIMING OF THE EXIT

The auditor should contact audit participants to determine a suitable time and location for the exit conference. The exit conference should be scheduled as soon as possible while taking into consideration the needs of the auditee.

DISCUSSION DURING THE EXIT

The discussion topics at each exit conference will vary depending upon several factors including audit concerns noted and the exit conference attendees. At a minimum, the auditor should be prepared to discuss the audit including what we did (i.e., objective, scope, procedures), what risks we perceived, how we anticipate the recommended action will address the associated risk, and other concerns identified.

For assurance or investigation engagements, if the auditee agrees with the wording and recommendations, the auditor should obtain an expected implementation date and the auditee's written agreement to implement the recommendation via a signature on the draft report at the exit conference, document agreement in the exit conference minutes, or obtain agreement via email. Sometimes language is proposed to better present the current state or proposed recommendation. Such changes can be discussed at the exit, and a revised draft should be shared with the auditee for approval.

If the auditee is not in agreement with the finding, audit management will continue to seek an agreement through the auditee's reporting line up to the audit report level (i.e., the individual to whom the report is being directed). If the individual to whom the report is being directed to does not agree to accept the recommendation and is willing to accept the risk of not implementing the recommendation, audit management will report the finding and risk acceptance within the final report. The following levels have been identified for risk acceptance concurrence and should be obtained prior to the issuance of the report.

- Low risk / priority recommendations may be risk accepted by the head or director of the unit in which the recommendation is made.
- Moderate risk / priority recommendations may be risk accepted by the head or director of the unit in which the recommendation is made with concurrence by that individual's supervisor (e.g., an academic department head's supervisor is the dean).
- High risk / priority recommendations may be risk accepted by the head or director of the unit in which the recommendation is made with concurrence by that individual's supervisor and the president, and vice-president (for U of I System) or chancellor (for university).

For consulting engagements, no formal agreement is necessary as any recommendations are optional, as previously agreed to by the auditee, and any implementation decision would rest with management unless another agreement was made.

PRE-APPROVAL OF HIGH RISK/PRIORITY RECOMMENDATIONS WITH A LONGER THAN ONE-YEAR PROPOSED TIMELINE

The president requires advance approval of any high risk/priority rated recommendation in the draft report where the auditee's proposed expected implementation date exceeds one year, along with auditee's rationale as to why implementation is planned to take longer than one year. This information will be provided by the auditee to the auditor. The executive director will communicate the draft report wording, expected implementation date, and the auditee's rationale to the president. Presidential approval of the auditee's expected implementation date is required prior to report issuance.

FINAL REPORT

Assurance and investigative audit reports will be distributed based on the reporting line of the unit all the way up the organizational hierarchy to the president of the U of I System, along with any applicable or responsible parties based on the report content. The report should be distributed to the individuals on the audit report distribution list as determined by the employees holding those applicable roles. E-mail transmittals for the distribution of audit reports must include the Illinois Freedom of Information Act disclaimer. In accordance with GIAS, all reports are issued by the executive director.

Consulting engagement reports will be distributed to the unit that has requested the consulting work. If significant risks are identified in a consulting engagement, the audit team should consider whether additional parties should be provided with a copy of the report. University or U of I System leadership can request copies. Unit leadership should be notified if additional distribution is deemed necessary and/or has been requested.

REPORTING AND FOLLOW-UP

FOLLOW-UP

FOLLOW-UP

Corrective action is the responsibility of management and is subject to follow-up in accordance with GIAS.

FOLLOW-UP PROCESS

Objective –
The objective of the follow-up process is to determine whether the audit concern has been effectively implemented, or management has accepted the risk of not taking action. When follow-up is performed, the auditor will find one of the following situations:

- Open – the corrective action has been initiated but is not complete; or the concern has not been addressed (if the auditor believes that the unit fully intends to address the concern, a new expected completion date should be entered, subject to the process described below).
- Implemented – the concern has been adequately addressed by implementing the original corrective action, or the concern has been adequately addressed by implementing an alternate corrective action.
- Partially Implemented – remaining risk accepted.
- Risk Accepted – if the auditor concludes that management has accepted the risk of not taking action and does not intend to implement the recommendation, notify audit management.
- Withdrawn – the concern no longer exists because of changes in the unit's processes.

Low Risk / Priority Recommendations –
We will perform one follow-up based on management's expected implementation date (the ABFFC's expectation is for management to implement within one year). If the auditee has not implemented the corrective action, the item will be closed as either partially implemented or risk accepted. Reporting will be included in the Quarterly Summary of Internal Audit Activity - Status of Audit Recommendations Table. No reporting of individual items to leadership will be made.

Moderate Risk / Priority Recommendations –
We will perform follow-up based upon management's original expected implementation date and if not implemented at that time, two additional follow-ups at dates established by management will be performed, with a total limit of two years for resolution. If, at the conclusion of three follow-ups or two years since the report was issued, management has not implemented the corrective action; the item will be considered to be risk-accepted and will be closed as either partially implemented or risk accepted. The closing of the recommendation as not implemented will be reported to leadership (including unit head, dean, vice chancellor, chancellor, vice president, president, and ABFFC). Through communicating these not implemented recommendations, leadership may determine lack of agreement with the risk-acceptance decision and direct management to implement. The method of follow-up to provide assurance on these recommendations will be determined on a case-by-case basis.

> **Partial Implementation and Moderate Risk Ranking Reduced –**
> In some situations, we may find that an original recommendation has been partially implemented to reduce the risk down to a low risk level. If this is the case, the recommendation should be closed as implemented, and documentation should be retained regarding the portion not implemented at the time of follow-up.

High Risk / Priority Rated Recommendations –
Any extensions beyond the original implementation date for a date that is longer than one year from report issuance will require approval by the president. If, at the conclusion of three follow-ups

management has not implemented or risk-accepted the corrective action, the item will be provided to leadership (including unit head, dean, vice chancellor, chancellor, vice president, president, and ABFFC). The chancellor or U of I System vice president must meet with the president and the executive director of University Audits to discuss. At the ABFFC's discretion, the same individuals must also meet with the ABFFC and the executive director of University Audits in closed executive session to discuss. The ABFFC and/or the president will either 1) agree to risk-accept the item or 2) permit management an extension and determine such date. If the item has not been implemented after the extended date, these same meetings and processes will take place until the item is closed as implemented, partially implemented, or risk accepted.

Partial Implementation and High Risk Ranking Reduced –
In some situations, we may find that an original recommendation has been partially implemented to reduce the risk down to a moderate or low risk level. If that has occurred, the remaining moderate or low risk should follow the guidelines for follow-up noted above for those risk categories. If the remaining moderate or low risk will be risk-accepted, the recommendation should be closed as implemented and documentation should be retained which would support notification of leadership as to the remaining risk.

Performance –
According to GIAS, internal auditors should confirm implementation of recommendations or actions plans by:

- Inquiring about progress on the implementation.
- Performing follow-up assessments using a risk-based approach.
- Updating the status of management's actions in a tracking system.

COMMUNICATION OF FOLLOW-UP RESULTS

Unit –
Follow-up results should be communicated by the auditor to the management team associated with the concern.

Leadership –
On a periodic basis, audit management reports to university and U of I System management, the ABFFC, and the full board various metrics regarding open and recently closed corrective action items. The decision of which action items to report is based upon input from the applicable leaders.

REPORTING AND FOLLOW-UP

ANNUAL REPORT

PURPOSE

The purpose of the Annual Report is to describe our service to the U of I System and demonstrate our accountability that the internal audit function is operating as intended, through the utilization of audit resources, performance metrics and benchmarks, and adherence to professional standards and our Internal Audit Charter. The Annual Report also satisfies the FCIAA requirement to submit to the president a written report detailing how the audit plan for that year was carried out, the significant findings, and the extent to which recommended changes were implemented. The Annual Report is also provided to the board as a Report for Information Only as part of the September board meeting materials, in advance of the September 30th FCIAA requirement. To protect the OUA's FOIA exemption, communication of significant findings is highly summarized in the publicly available Annual Report and is provided in more detail through the ABFFC presentation and quarterly reporting to the president and ABFFC.

PERSONNEL

PERFORMANCE APPRAISAL PROCESS

OVERVIEW

The OUA adheres to the annual U of I System performance appraisal process. Performance appraisals provide employees and their supervisors an opportunity to establish goals, identify areas in which they have excelled, and document areas which are in need of more focus. The executive director or director (supervisor) initiates the annual performance appraisal process.

The performance appraisal system can be accessed at: https://hrnet.uihr.uillinois.edu/UHR/PerformanceAppraisal/index.cfm (this site requires enterprise authentication login).

Continual feedback is provided on an informal, continual basis throughout the year as part of the audit review and comment process. More formal evaluations may be provided in an ad-hoc manner as determined by the executive director or director(s).

PERSONNEL

TRAINING AND PROFESSIONAL DEVELOPMENT

GENERAL

Each auditor should possess a body of specialized knowledge and maintain a recognized, continuous process of education to sustain continuous professional growth in the field of Internal Auditing. Below are the CPE requirements of the SIAAB, Certified Internal Auditors (CIA), Certified Information Systems Auditors (CISA), and Certified Fraud Auditors (CFE). Funding for courses, training, and memberships is subject to budgetary constraints and director approval.

STATE INTERNAL AUDIT ADVISORY BOARD REQUIREMENTS

In compliance with the requirements established by the SIAAB, Article II, Section V *Bylaws, Section V – Continuing Professional Education Requirements*, all internal auditors must complete a minimum of 80 hours of CPE that directly enhance the auditor's professional proficiency to perform audits or attestation engagements. At least 24 of the 80 hours of CPE should be in subjects directly related to government auditing, the government environment, or the specific or unique environment in which the U of I System operates. At least 20 of the 80 hours must be completed in any one-year of the two-year period. At least 4 of the 80 hours of CPE must be in subjects related to ethics. The 80 hours of CPE, 24 hours of government CPE, and 4 hours of ethics CPE must be satisfied during two successive (non-rolling) calendar years. Internal auditors hired after the beginning of our 2-year CPE period should complete a prorated number of CPE hours based on the number of full 6-month intervals remaining in the CPE period.

It is the OUA policy to ensure that each auditor meets the CPE requirements.

CIA REQUIREMENTS

Effective January 1, 2013, CIAs performing internal auditing functions must complete a total of 40 hours of acceptable CPE every year. At least 2 hours each year should be in ethics.

For additional information on CIA requirements go to the IIA website:
https://www.theiia.org/en/certifications/already-certified/cpe-requirements/
https://www.theiia.org/en/learning/ethics-resources/

OTHER CERTIFICATION

Other certifications that are held may be tracked in K-10, at the auditor's discretion.

CPE RECORDS

Auditors are responsible for recording their CPE activity for the SIAAB and CIA in K-10. This includes attaching any applicable supporting documentation. CPE sponsored by the OUA will be entered in K-10 by the OUA prior to distribution of the certificate.

Required records for CPE participation shall be maintained for at least six years.

TUITION WAIVERS

Subject to U of I System rules and regulations, staff members may receive tuition waivers for U of I System courses. See U of I System policies at https://www.hr.uillinois.edu/benefits/tuitionwaivers. Release time may be granted for job-related courses, subject to the needs of the department, in

accordance with the U of I System rules and regulations. Staff members are encouraged to participate in advanced degree programs that will assist in the career advancement goals; however, such courses are generally required to be taken after work hours or using available vacation hours. Educational activities require pre-approval by your director. Departmental needs and budget availability will be included in the approval decision.

PROFESSIONAL CERTIFICATION EXAMS AND MEMBERSHIPS

Staff members are encouraged to prepare and sit for the examinations for professional certification such as Certified Public Accountants (CPA), Certified Internal Auditors (CIA), Certified Fraud Examiner (CFE), and Certified Information Systems Auditors (CISA). Preparation for professional certification may be carried out through self-study, U of I System courses, other university or college courses, professional society courses, or specialized review courses. Release time may be granted in accordance with the process noted regarding tuition waivers. Examination/registration fees will be reimbursed after successfully passing the exam. Invoices for fees should be submitted to audit management. The policy on memberships in professional organizations paid for by the OUA is:

1. All professionals are provided IIA memberships (including local chapter) as a Government Member.
2. Other professional memberships may be supported for those holding professional certifications in professional organizations promulgating the certification.

ADMINISTRATIVE PROCEDURES

COMPUTERS

INFORMATION SECURITY

Data Ownership: All data kept on OUA computers and networks should pertain to the U of I System and related professional duties of the audit staff. As such, these files are considered the property of the OUA, rather than the property of the individual who has created them.

ACCEPTABLE USE OF COMPUTING AND NETWORK RESOURCES

U of I System office employees must comply with the guidelines outlined in this policy. It is the employee's responsibility to thoroughly review this policy which is available at UA Mobile Computing Guidelines.

HANDLING COMPUTER/NETWORK PROBLEMS

Computer, application, or network problems from all three universities will be handled as follows:

1. K-10 issues will be handled by an internally designated contact person.
2. All other computer, application, or network issues and problems need to be reported through the AITS service desk. See:
   https://www.aits.uillinois.edu/services/application_services/service_desk
   https://www.aits.uillinois.edu/get_help

ADMINISTRATIVE PROCEDURES

AUDITOR TIMEKEEPING

The OUA maintains records of usage of benefit time and time spent by day in accordance with the U of I System policy. The OUA also records all time, including time spent by audit or project, in K-10 to assist in reporting audit coverage, planning of future audits and projects, and evaluating audit staff and audit plan completion. At the end of each week, all staff are required to enter time into K-10.

RECORDS RETENTION POLICIES

RECORDS DISPOSITION AUTHORIZATION

A Records Disposition Authorization, Application #UI-01-10, for the OUA was filed with the Office of the Secretary of State, October 8, 2001, and approved by members of the State Records Commission at their November 21, 2001, meeting. This authorization allows the OUA to dispose of, or transfer to the State Records Commission/Archives, the records listed below.

AUDIT REPORTS FILES – FISCAL YEARS 1976-PRESENT

Audit reports are retained in electronic format for a period of 20 years from audit completion (report issuance). Pre-fiscal year 1997 reports are maintained in TIFF format. Post fiscal year 1996 files are maintained in HTML or ASCII format. Backup (redundant) copies of all files are maintained during the 20-year retention period. Audit reports that have reached the 20-year retention period are forwarded to the university archivist (archivist) in a non-proprietary format such as PDF.

WORKPAPER FILES – FISCAL YEARS 1996-PRESENT

All audit workpapers are retained for a period of 10 years from audit completion (all issued recommendations have been closed). Workpapers are retained in electronic format. Backup (redundant) copies of all workpaper files are maintained during the 10-year retention period. Software and hardware able to read all files is maintained during the retention period, or electronic files are translated to a format which may be ready by current software and hardware. At the end of the 10-year retention period, workpapers may be destroyed in accordance with the Records Disposal section below.

GENERAL CORRESPONDENCE FILES

General correspondence files include final, formal correspondence outside of the K-10 (previously AutoAudit) process such as routine correspondence, copies of U of I System reports generated by other offices, and memoranda relating to university committees on which audit staff serve. These files may be destroyed after a period of 5 years in accordance with the Records Disposal section below. However, correspondence pertaining to the charge, mission, and activities of the OUA is considered to be historical record. Historical records that have reached the 5-year retention period are forwarded to the archivist.

OTHER RECORDS

Other OUA records are to be retained in accordance with other U of I System related policies. See: https://www.busfin.uillinois.edu/bfpp/section-13-accounting/keeping-accounting-records

RECORDS DISPOSAL

Records may only be disposed of upon authorization of the State of Illinois through the Records and Information Management Services (RIMS) office, in accordance with the State Records Act.

EXTERNAL CONSULTANTS (consultants)

Some audit assignments are quite technical, have technical aspects, or require specialization. A thorough audit may require the services of technical or specialized consultants.

Audit management is responsible for acquiring and monitoring the services of a consultant to ensure that the FOIA protection for internal audits applies. The executive director must approve the use of a consultant prior to requesting these services. Consultants may be used for the duration of an assignment or on an as-needed basis.

ADMINISTRATIVE PROCEDURES

DRESS CODE

Staff will be expected to dress in a manner consistent and appropriate to their business activities and schedule each day. If meetings are held with outside parties, auditors should conform to the dress code expected for other meeting attendees. If you do not know what to expect, then professional dress should be chosen.

Casual dress is acceptable if a staff member does not have any meetings with external clients. Discretion and good judgment should guide staff not to wear anything that is offensive, distracting, or overly casual.