
MANUAL
INTERNAL
AUDIT
TEMPLATE

Internal Audit Manual Template

TABLE OF CONTENTS

POLICY

INTERNAL AUDIT CHARTER

POLICY

MISSION STATEMENT

The mission of the Office of XXX Audits (Office) is to provide independent and objective services to protect and strengthen the XXX System (System) and its related organizations.

VISION STATEMENT

Be an innovative driver of positive change while striving to be the premier audit function in higher education.

GUIDING VALUES

We perform all that we do with:

- Objectivity
- Independence
- Integrity
- Confidence
- Credibility
- Leadership
- Straightforwardness
- Excellence
- Innovation
- Professionalism

STRATEGIC GOALS

1. Our Office will continue to cultivate relationships and understanding through communication with the BOD and senior leadership of the System.

2. Serve as counsel to the BOD, the xxx, management, and other constituents.

3. Enhance audit efficiencies and effectiveness.

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 IIA Standards.

QUALITY

Quality in an audit is achieved when:

- The audit results in a positive impact on processes where such an opportunity exists.
- There is good communication between auditor and auditee and between the auditor and audit management.
- The perspective and needs of the auditee are incorporated into the audit process.
- The audit objectives, scope, and procedures are constantly reassessed to ensure efficient use of audit resources.
- Audit objectives are achieved in an efficient and timely manner.
- Audit work is adequately documented.
- Auditees have an opportunity to review our findings, conclusions, and recommendations as we strive for mutual agreement.
- Other applicable professional standards are met.

PRODUCTS

Our primary output is the independent analysis and recommendations necessary to assist management in improving administrative functions. This is achieved through our interaction with our auditees, through our interaction with the System community, and by our:

- Audit Reports – issued to the President, Vice President and Chief Financial Officer, applicable Chancellor, and operating management.
- Management Communications (e.g., letters, memos, e-mail) - issued to operating management.
- Support for the President's Internal Control Certification – issued to the President and Director of Financial Services.
- Annual Report – issued to the Audit, Budget, Finance, and Facilities Committee of the BOD, the President, and all senior administrators participatingin the audit planning process.
- Two-Year Plan – issued to the Audit, Budget, Finance, and Facilities Committee of the BOD and President.

POLICY

STATE OF XXX
FISCAL CONTROL AND INTERNAL AUDITING ACT

The Fiscal Control and Internal Auditing Act (XXX Compiled Statutes, 30 ILCS 10/1001) (XXX) is thestate legislation which provides guidance and mandates for internal audit activities of State agencies.

The State Internal Audit Advisory Board (Board), as established by XXX, is responsible for promulgating a uniform set of professional standards and a code of ethics to which all State internal auditors must adhere. These requirements are included in the Board'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 the Board as provided by XXX. These Standards shall be summarized in the Quality Assurance Matrix on the Board's website. These Standards include *The Institute of Internal Auditors International Professional Practices Framework.*

Article II, Section IV, Code of Ethics, states that "All State auditors shall adhere to standards of conduct which were derived from the *Code of Ethics* published by the Institute of Internal Auditors."

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 XXX System (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.

Confidential information acquired by audit staff through their employment is considered to be privileged and must be held in strictest 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 System purposes and not 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 System. Confidential information is transmitted only to those persons who need the information to discharge their duties as System employees or audit staff. Any other dissemination of work paper 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.

Prior to disposal, all paper documents generated in the course of performing audit work must be shredded.

The following standard e-mail disclaimer must be used for all messages distributed outside of the audit office:

> Materials prepared or compiled by internal audit activities of public bodies, including e-mail communications relating to internal audit activities, **are exempt** from the XXX Freedom of Information Act.

It need only be used on the first e-mail in a communication string. For subsequent responses, there is no need to repeat the signature tag.

REPORT SECURITY AND CONTROL

Access to audit reports and management communications is restricted to authorized audit staff. Audit reports are available to all audit staff from the electronic copies maintained on the Office of XXX Audits computer network.

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

CONFIDENTIALITY STATEMENT

On the first day of employment staff must sign the following statement. (*Statement should be on office letterhead in memo format*.)

TO: (Staff Member)

FROM: (Audit Management)

DATE: (Date)

SUBJECT: Confidentiality

During the course of any job duties, employees of the Office of XXX Audits may have access to information that is sensitive, nonpublic, or protected by Federal or State privacy statutes. All information contained in audit work papers and audit reports or disclosed to auditstaff is confidential.

It is the policy of the Office of XXX Audits not to disclose to anyone outside the XXX System (System) the contents of any audit work papers, audit reports, or other information made available by the System. Disclosure within the System will be only forjob-related purposes and only to those who, in the audit staff's judgment, have a need to know.

I have received, read, and understand the Office of XXX Audits' confidentiality policy. I understand that it is a condition of my employment to adhere to the confidentiality policy, and that violation of this work rule may result in disciplinary action including dismissal.

_____ _____

Signature Date

POLICY

INDEPENDENCE AND OBJECTIVITY

Per IIA Standard 1100 – Independence and Objectivity, "The internal audit activity must be independent, and internal auditors must be objective in performing their work. Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner." They must have no authority over or responsibility for the activities they audit. "Objectivity is an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made."

The Office's organizational independence is demonstrated through the Organization Chart and Internal Audit Charter.

In order 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 XXX Policy on Conflicts of Commitment and Interest
2. Any activity that the auditor previously performed or supervised unless a reasonable period of time has elapsed.
3. Any other situation in which a conflict of interest or bias is present or may reasonably be inferred.

If through your actions or state of mind your audit objectivity is or can be inferred to be impaired, notify audit management immediately. To assist in recognizing potential or perceived areas of conflict of interest, an Auditor Independence form will be completed by auditors on the first day of employment and annually thereafter. (Statement should be on office letterhead in memo form.)

AUDITOR INDEPENDENCE AND OBJECTIVITY

To assist in recognizing potential or perceived areas of conflict of interest or objectivity impairment, please complete the following questionnaire, sign, and give to your appropriate Director for signature and return to me by **[enter date]**.

Area where relative[1] works: (Please write "None" if not applicable.)	Relative's relationship to you, title, and general description of job related duties:
_____	_____
_____	_____
_____	_____

Area(s), other than already listed above, where you feel your objectivity could be impaired or inferred impaired:

Area: (Please write "None" if not applicable.)	Reason: general description of job related duties:
_____	_____
_____	_____
_____	_____

_____ _____
Employee Signature Date

Reviewed By:

_____ _____
Director Signature Date

_____ _____
Executive Director Signature Date

[1] Relative = Immediate Family as defined by the XXX Policy on Conflicts of Interest and Commitment

POLICY

XXX NONDISCRIMINATION STATEMENT ANDSTATEMENT ON SEXUAL HARASSMENT

XXX Nondiscrimination Statement

XXX Statement on Sex Discrimination, Sexual Harassment, and SexualMisconduct

Section Revised: 12/18/15

POLICY

QUALITY ASSURANCE

GENERAL

The establishment and implementation of a quality assurance and improvement program for the Office is required by the *Standards* and includes both internal and external assessments. Per the *Standards*, "A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the Definition of Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for 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. The State Internal Audit Advisory Board (SIAAB) requires a periodic self-assessment whenever there is a significant change in personnel or auditing standards; the self-assessment must be completed after allowing a reasonable period of time for implementation. Self-assessments must be completed utilizing the SIAAB Quality Assurance Matrix. The internal assessments should typically be performed by an experienced auditor, audit management, or combination thereof.

The results of self-assessments are communicated to the VP-CFO; President; and Audit, Budget, Finance, and Facilities Committee upon completion and the results of ongoing monitoring are communicated at least annually. The results of ongoing monitoring are typically communicated via quarterly and annual reporting to the VP-CFO; President; and Audit, Budget, Finance, and Facilities Committee.

EXTERNAL ASSESSMENTS

In compliance with The IIA *Standards* and *SIAAB Bylaws*, an external assessment of the Office will be performed every five years by a qualified, independent assessor or assessment team from outside the XXX. The Executive Director discusses with the President and Audit, Budget, Finance, and Facilities Committee the qualifications and independence of the external assessor or assessment team, as well as the whether the form of the external assessment is to be a full external assessment or self-assessment with independent validation. The results of external assessments are communicated to the VP-CFO; President; and Audit, Budget, Finance, and Facilities Committee upon completion.

AUDIT PLANNING

ANNUAL AUDIT PLANNING

OVERVIEW

Each year, a two-year audit plan of XXX System (System) audits is submitted by the Executive Director of XXX Audits to the President of the System andthe Chairman of the Audit, Budget, Finance, and Facilities Committee of the BODfor approval. In accordance with XXX, 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 System's goals. Audit office management, as well as audit staff at the direction of their Director, participate in the annual audit planning process. Development of the plan takes into account the System's Strategic Framework, risk management framework, Office management's judgment of risks, and input from senior management and the Audit, Budget, Finance, and Facilities Committee (ABFFC).

XXX requires the two-year plan to include:

- Audits of major systems of internal accounting and administrative control such that each cycle is addressed every two years. Due to the System's multi-faceted, decentralized structure, these audits are performed using a combination of the XXX Comptroller 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. Major systems, as defined via the SAMS Manual are:

    - 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

- Audits of 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 for 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.

RISK CATEGORIES

Categories of risk we assess include the following:

- Financial – Financial risks deal with the internal controls over and reporting of financial transactions, including assets, liabilities, revenues, and expenditures.
- Compliance – Compliance risks deal with the adequacy of a unit's system of internal controls to ensure compliance with applicable laws, regulations, and policies.
- Operational – Operational risks deal with the unit's ability to use its resources in an effective and efficient way.
- Reputational – 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 – Safety risks include events, situations, or other circumstances that have the potential to cause harm to individual(s), including students, employees, and the public.

KEY ELEMENTS OF THE AUDIT PLAN DEVELOPMENT PROCESS

- Define the Audit Universe – The audit universe is multi-dimensional. It considers:
    - Units – all Banner orgs
    - Business processes
    - Compliance topical areas
    - Strategic risks identified through the Enterprise Risk Management process
    - Other current and emerging issues

- Review the System's Strategic Framework, including current business plans and strategies

- Identify and summarize the key risks across the System
    - Perform data analytics on all Banner orgs to translate selected risk areas into measureable risk factors, and rank by risk
    - Identify key stakeholders and meet to discuss their plans, issues and risks in achieving their business objectives
    - Review the System's Strategic Framework, including strategic risks as identified through the Enterprise Risk Management process
    - Review and coordinate with efforts of XXX Ethics and Compliance Office
    - Consider other factors such as:
        - External audit findings
        - Federal funding source audit plans
        - Higher education industry issues
        - Other regulatory or standards changes
        - Length of time since previous audit

- Develop an audit plan based on assessed risks. The plan is comprised of:
    - Planned audits
    - Allocation of hours for follow-up
    - Reserved hours for special projects, investigations, and other unplanned projects

- Map the key risks into the audit plan to determine if:
    - The issues are already appropriately covered by the planned program. In doing so, consider where the focus within existing audits could or should change
    - New audits need to be developed to focus on the issues and risks identified and add these audits to the audit plan

- Review the audit plan with those charged with governance.
    - Discuss the expectations of senior management, the XXX, and other stakeholders for internal audit opinions and other conclusions
    - Solicit their input as to whether they believe the audit plan appropriately covers identified risks

- Obtain the System President's approval of the two-year audit plan on or before June 30.

AUDIT PROCESS

OVERVIEW

TYPES OF AUDITS

Internal control audits determine whether the unit is conducting its financial and business processes under an adequate system of internal control, as required by the XXX System (System) policy and guidelines and good business practice.

Compliance audits determine the adequacy of a unit's system(s) designed to ensure compliance with 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. Audit recommendations typically address the need for improvements in procedures and controls intended to ensure compliance with applicable regulations.

Financial audits attest to the accuracy of financial information of assets, liabilities, revenues, expenditures, or other financial presentations.

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

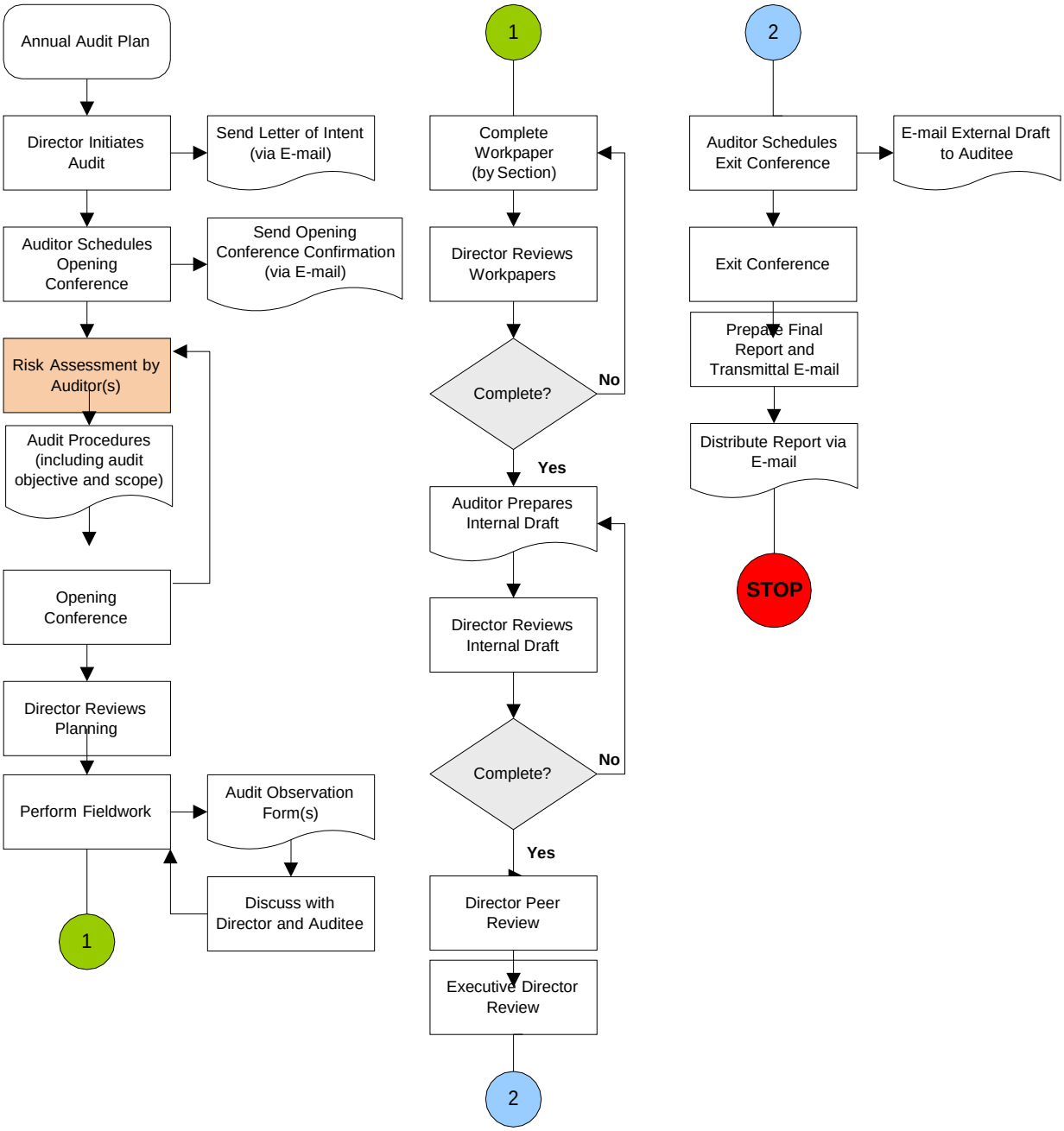
Operational audits examine the use of unit resources to evaluate whether those resources are being used in the most efficient and effective ways to fulfill the unit's mission and objectives. An operational audit can include elements of a compliance audit, a financial audit, and an IT audit.

Investigative audits focus on alleged civil or criminal violations of state or federal laws or violations of System policies and procedures that may result in prosecution or disciplinary action. Allegations of theft or misuse of System assets, white-collar crime, and conflicts of interest are examples of issues addressed by investigative audits.

Continuous auditing is a method of analyzing data with the objective of assessing risk and related internal controls. It involves using various data analysis techniques to identify anomalies and other indicators, such as non-compliance with System policies, which may reveal control weaknesses. It can be used to assess the risk of a particular business cycle or to identify non-compliance. The analysis can be 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.

Consulting and Advisory Services are management related service activities. 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.

This section of the manual explains the steps for conducting an audit from the initial assignment through fieldwork. Similarly, the reporting and follow-up processes are covered in a separate section of the Manual. A flowchart of the audit process follows.



7

AUDIT PROCESS

AUDIT ASSIGNMENT

ASSIGNING THE AUDIT

Each Director assigns audits to each individual auditor on their staff. The Completion Table within AutoAudit is completed by the Director and any planning comments are noted. Information is provided to the auditor including the preliminary objectives or type of audit, general scope of the audit, if known, and any additional information that is needed (reference material available, what to watch for in certain tests, problems noted during other audits, information about who requested the audit and why, the area of responsibility, etc., so the auditor can begin the risk assessment process).

AUDITEE NOTIFICATION

Certain audits, such as investigative audits, may not be announced. Otherwise, if the auditee is not already involved in the request or scheduling of the audit, the Director will notify the auditee via e-mail, prepared by the auditor, that an audit of their unit has been scheduled. The message should explain that the auditor will contact the auditee to arrange an opening conference.

The auditor will draft the email using the template "Format for Letter of Intent E-mail" in Auto Audit's Standard Library (Maintenance Menu, Standard Library Menu, Audit Formatsview).

AUDIT PROCESS

RISK ASSESSMENT PROCESS

Audit management provides the draft audit objective(s), the hours budgeted for the project (included in the Two-Year Plan), and other pertinent information to the auditor. The risk assessment process starts with the auditor's identification and analysis of risk for an audit based on the objective provided by management.

The Standards state:

- Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

- Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

- Adequate criteria are needed to evaluate governance, risk management, and controls.

- Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management and/or the board to develop appropriate evaluation criteria.

- 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.

Depending on the audit type, the auditor needs to consider:

- The mission and objectives of the unit or process under review.
- The organizational structure of the unit and the related XXX or XXX System (System) Administration structure from reviewing the unit's organization chart.
- The probability of significant errors, irregularities, noncompliance, and other exposures that would adversely affect the unit's operations and/or their ability to efficiently and effectively accomplish their objective or would adversely affect the System's overall mission/objective.
- Key financial and administrative data relevant to the audit from BANNER, sub ledgers, or other unit reports.
- Unit, XXX/System, and other applicable standards (e.g., NCAA Legislation, JCAHO standards) for measuring critical functions.
- Control processes either existing or expected to monitor critical functions for compliance with established standards.

- Issues and concerns raised in prior audits of the unit.
- Management's concerns and input regarding risk.

Using professional judgment and available information, determine the most appropriate audit scope (e.g., statement of audit boundaries) and any changes recommended for the objective. Determine if the recommended scope/objective will change the budgeted hours and propose a new budget, if necessary. Develop and document planned dates for the completion of the audit. When completed, submit for audit management's approval the most appropriate audit objective(s) and scope to define a statement of audit boundaries.

Based on the information gathered above, select the appropriate audit approach. Consider:

- The evidence necessary to reach conclusions on audit objectives.
- The tests and other procedures to be performed to gather the required evidence.
- The objectives, steps, and procedures so that the high risk processes are performed first.

This will assist the auditor in keeping focused on completing the audit by developing sufficient information to report on the audit early in the process. If necessary, the audit can be ended (e.g., as a result of revised objectives, budget changes, new audit requests), before all of the originally anticipated procedures are performed.

When determining what audit procedures to perform, the auditor should review the standard audit procedures, maintained in the "grey tab" in Auto Audit to determine whether there are established procedures in place to address the area of concern. If so, the auditor should chose the standard procedures and, if necessary, modify to address any concerns specific to the audit.

If standard procedures are not available for the topic, the auditor will need to develop procedures specific to the area. Audit procedures should be organized in the following manner:

Audit Procedures	**Results/Doc Link**	**Initials**
Audit Objectives:		
Scope:		
Audit Step 1:	Conclusion:	
Procedures Performed		
Audit Step 2:	Conclusion:	
Procedures Performed		
Audit Step 3:	Conclusion:	
Procedures Performed		

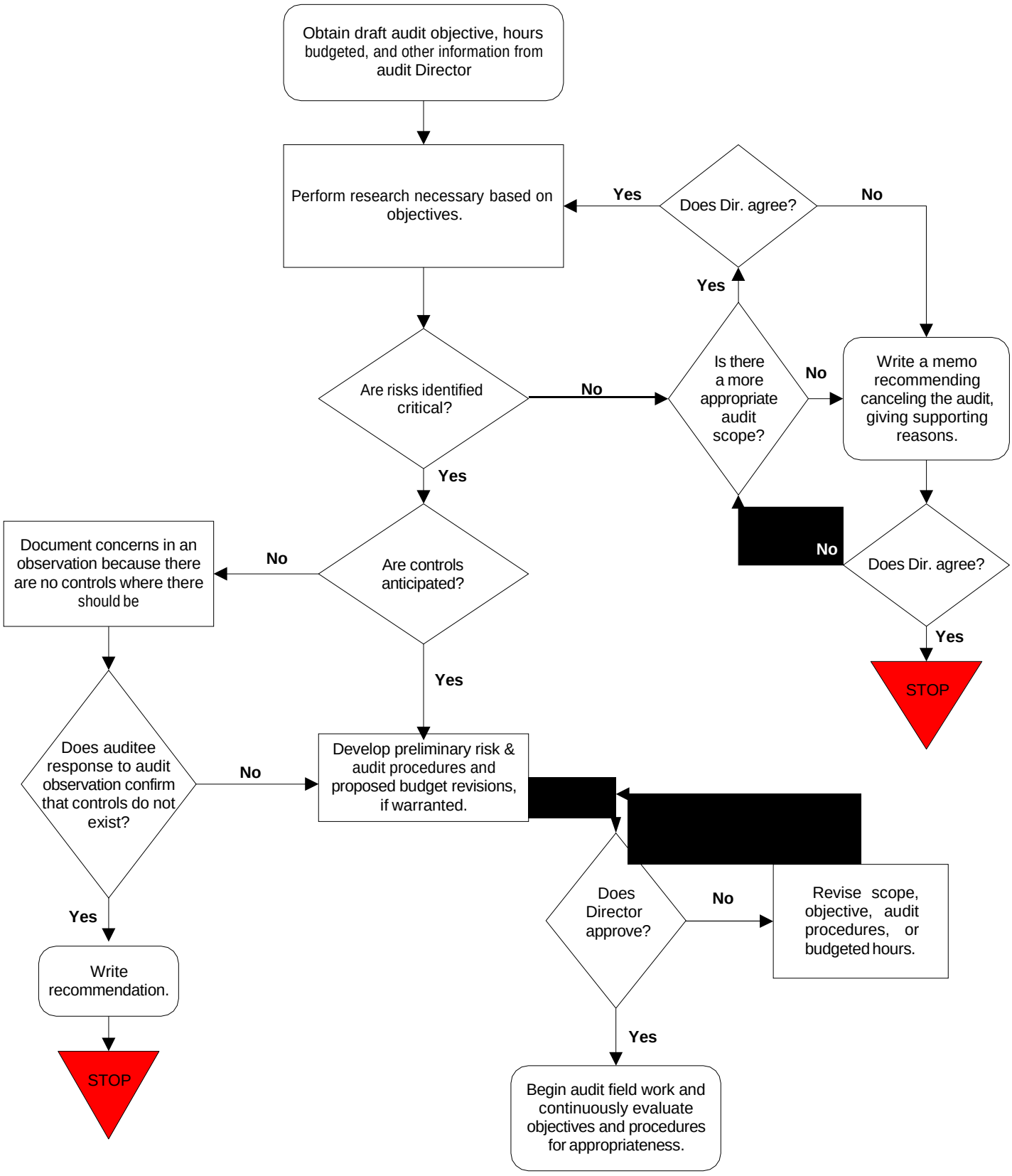
Prepare audit procedures and submit for audit management's approval. Audit procedures provide detailed audit steps to be performed during the audit fieldwork that will achieve the specific audit objectives.

If, subsequent to the approval of audit management, a decision is made not to perform one or more of the standard procedures, a note documenting the reasons for the decision should be included in the audit procedures.

During the course of the audit, conditions may arise which warrant revising the audit procedures, scope, or budgeted hours. The auditor should evaluate the situation, make timely recommendations to audit management, and obtain approval before incorporating any changes.

The following flowchart of the risk assessment process is provided to further illustrate the process.

RISK ASSESSMENT PROCESS FLOWCHART



AUDIT PROCESS

OPENING CONFERENCE

The opening conference should be held to explain the audit process and gather any initial information regarding the auditee. Under some conditions, the objective and scope may be predetermined and should be communicated and discussed at the opening conference. If the objective and scope have not been predetermined, the process for making that decision and how it will be communicated should be discussed. The auditor should prepare an opening conference e-mail confirming the appointment. The e-mail should briefly state the announcement of the audit; the date, time, and place of the opening conference; the purpose of the opening conference; and the desire to resolve any questions about the audit.

Certain audits, such as investigative auditor requested audits, may not have an opening conference.

The opening conference is an important step in a regular audit. It is an opportunity to establish the proper tone and to begin building good relationships. Explain the "who, what, where, when, why, and how" for those who have not been exposed to the audit process.

During the opening conference:

1. Provide and discuss the Office brochure (optional).
2. Emphasize that the purpose of an audit is to help improve XXX System controls and operations.
3. Review the objective(s) and scope of the audit, encouraging management to discuss any aspect of the audit.
4. Ask for suggestions of potential auditee problem areas within the audit scope. This communicates an intention of being helpful rather than critical.
5. Determine what assistance from personnel other than those attending the opening conference is needed to answer detailed questions concerning the functions to be performed.
6. Explain how audit concerns (observations) are handled. Explain that concerns will be reviewed with the designated auditee at the time they arise and identify who will be responsible for reviewing the audit concerns. Explain the purpose of discussing each audit concern is to verify that both the facts defined in the concern and the impact of the concern are accurate. Some findings may be resolved verbally.
7. Establish how frequently the department head/director wants to be updated on audit progress and findings.
8. Explain we will review the draft audit report in detail at the exit conference.
9. Explain that a copy of the final audit report will be sent to their reporting line up to and including the Chief Financial Officer and the President.
10. Inquire about working hours, working area, access to records, and any other information that details the office routines.
11. Identify information needed to complete the audit procedures.
12. Establish a tentative schedule for the audit process.

13. Ask if there are any questions concerning anything discussed at the opening conference or any questions in general about the auditor or audit approach that will assist the auditees in their understanding of the audit project.

Effective communication at the beginning of the audit can materially influence the tone in which the entire audit is conducted.

OPENING CONFERENCE MINUTES

The Opening Conference's date, attendees, and substantive items discussed which are directly related to audit scope, objectives, timing, or confidentiality should be documented in the work papers.

The template of the Opening Conference Email and Opening Conference Discussion Items are in the Standard Library section of Auto Audit.

AUDIT PROCESS

FIELDWORK

DEFINITION AND PURPOSE

Fieldwork is the process of gathering evidence and analyzing and evaluating that evidence. The methods of gathering evidence and analyzing should be described in the audit procedures developed by the auditor and approved by management. If possible, the audit objectives and procedures should be performed so that the most important and significant audit steps are completed first. Fieldwork should be documented in workpapers as the work is being conducted.

Throughout fieldwork, professional judgment should be used to: a) determine whether evidence gathered is sufficient, relevant, competent, and useful to conclude on the established objectives; 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). Document changes in audit objectives, scope, and procedures in the work papers.

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 accounting, business, and other operational records.
5. Analyzing data and information.
6. Reviewing systems of internal control and identifying internal control points.
7. Evaluating and concluding on the adequacy (effectiveness and efficiency) of internal controls.
8. Conducting compliance testing.
9. Conducting substantive testing.
10. Determining if appropriate action has been taken in regard to significant audit concerns and corrective actions reported in prior audits.
11. Discussing potential risks and recommendations with the auditee and the cost/benefit assessment that led to recommendations.

Guidelines for documenting fieldwork (e.g., the evidence gathered, the analyses made, the tests performed), to support the findings and conclusions are presented in the sections Work papers and Audit Observations.

Fieldwork should be performed at the auditee's location to facilitate communication with the auditee. The auditor should maintain contact with auditee management and keep them informed of the audit observations and other developments throughout the audit. They may be able to provide additional information or may wish to adopt recommendations quickly.

AUDIT PROCESS

WORKPAPERS

WORKPAPER PREPARATION

The auditor documents work performed in AutoAudit. The work papers are the connecting link between the audit assignment, the auditor's fieldwork, and the final report. Work papers contain the records of the planning and risk assessment process, audit procedures, fieldwork, and other documents relating to the audit. Most importantly, the work papers document the auditor's conclusions and the reasons those conclusions were reached. The disposition of each audit observation identified during the audit and its related corrective action should be documented on an Audit Observation Form within AutoAudit. Work papers should be completed throughout the audit. As each meaningful section is completed, the auditor should submit the related work papers for review. The workpapers provide the basis for supporting our conclusions and engagement reports, as well as evaluating the Office's quality assurance program to demonstrate the Office's conformance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

Workpapers should be economical to prepare and to review. It is easy to include every scrap of information and every form in the work papers. However, the workpapers then become a confused mixture of data that is difficult to assimilate and use. Workpapers should be complete but concise -- a usable record of work performed. Auditors should include in their workpapers only what is essential; and they should ensure that each workpaper included serves a purpose that relates to an audit procedure. Workpapers that are created and later determined to be unnecessary may be deleted. Workpapers should be clear and understandable. The auditor should keep in mind that other people will examine and refer to the workpapers. The workpapers should not need any supplementary information and should stand-alone. An experienced auditor reviewing the workpapers, without referring to documents outside of those included in the workpapers and without asking questions, should be able to identify what the auditor set out to do, what they did, what they found, and what they concluded. Conciseness is important; but clarity should not be sacrificed just to save time and space.

See ***Appendix A*** for Office of XXX Audits Workpaper Guidelines.

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 and have a useful purpose, evidence the audit work performed, and sufficiently support the audit findings. In addition, the auditor should ensure the conclusions reached were reasonable and valid, and that Office workpaper guidelines were 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 should be returned/destroyed upon the completion of the audit.

Audit Management

Approval should be documented at the time the risk assessment process, audit procedures, and workpapers are reviewed. This approval is recorded by using the approval function within AutoAudit. It is important to document appropriate and timely management supervision. All workpapers should be independently reviewed to ensure there is sufficient evidence to support conclusions and all audit objectives have been met. A comprehensive review will be conducted by audit management before approving the draft audit report.

Audit management will:

- Determine compliance with work paper guidelines.
- 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 work papers to ensure they support the procedures performedand all procedures have been completed.
- Determine that the work papers adequately document the conclusions reached in thereport.
- Confirm that all observation forms prepared have been discussed with the appropriate member of management, and that the disposition of the audit concern is documented.

Document review comments by using the comment form within Auto Audit. When review comments have been satisfactorily cleared in the audit work papers, audit management willremove the comments from the work papers.

Upon completion of the Audit Report Checklist audit management will close the audit in the Auto Audit Overview document using the current date.

HOW TO USE AND RETAIN PERSONAL HEALTH INFORMATION (PHI) IN WORKPAPERS

When working with personal or patient health information data, the auditor needs to consider what evidence to include in the work papers. The decision point for including PHI is to first determine if it is necessary to evidence the audit work performed. The data elements considered to be personal identifiers are listed in ***Appendix B***. Workpapers should not contain any of the elements listed on ***Appendix B***. Instead of de-identifying the data in or attached to the workpaper, the XXX created a secure Box environment for the storage of PHI. Each audit containing PHI as audit evidence will have the data identified and the audit artifact storedin a uniquely named subfolder in the secured Box environment. The placement of the audit artifact containing PHI should occur concurrently with the audit.

If it is necessary to use XXX in your audit please ask your Director to create an audit specific filein the XXXX Work papers secured Box folder and give you access. The unique file should be named [Box Health – Internal} XX-XX-XXXXXX-X Audit Name or other unique name. The Xs represent the standard naming convention used for titling audits. The first two Xs are the XXX business transaction cycle. The second two Xs are the last two digits of the fiscal year. The next six Xs are the Banner organizational level 5 or program level 3 code. The last X represents the number of times the unit was audited in the fiscal year. If the numbering convention is not used, the unique title of the audit should be used to identify the audit.

The storage of PHI in Box of embedded text or attachments should occur as the workpapers are being prepared. PHI should not be retained in the Auto Audit production database.

The title of the file in the particular audit should identify the workpaper number and name of the attachment or a description of what embedded text is being cut out of the audit artifact. Working with attachments are easier than embedded text. A placeholder is inserted at the point in the workpaper where an audit artifact was removed. The placeholder is:

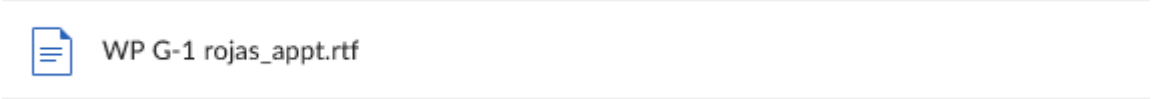
This audit artifact contains Electronic Protected Health Information and is stored in the University's Health Data Folder repository. If you require access to this artifact, please contact the Director of the Office of University Audits

If the removed item is an attachment, open the attachment, select 'Save As' and keeping the same file name insert the workpaper number or name before the file name and save the file to your desktop. Drag the file to the audit specific Box folder and ensure it uploads. Delete the file from your desktop and empty your recycle bin. Go back into Auto Audit, right click the attachment and select Delete. This will insert a message the auditor deleted the titled attachment. ***Example 1a*** as it appears on the workpaper:

This audit artifact contains Electronic Protected Health Information and is stored in the University's Health Data Folder repository. If you require access to this artifact, please contact the Director of the Office of University Audits.

[attachment "rojas_appt.doc" deleted by ncrowley/Audits/central/UIllinois]

Example 1b as it appears in Box:



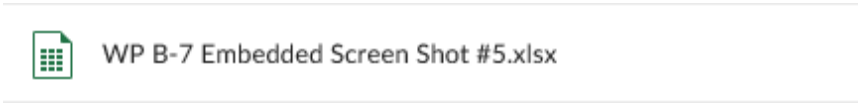
If the item is embedded text, the placeholder is inserted and the text cut out and placed on an Excel or Word document and create a header identifying the item(s) and paste them in. On the workpaper create a reference to indicate the removed item. Ideally, the reference on the workpaper is titled the same on the document created to paste the embedded text. ***Example 2a*** and ***2b*** depict the audit artifact in Auto Audit and Box.

Example 2a:

This audit artifact contains Electronic Protected Health Information and is stored in the University's Health Data Folder repository. If you require access to this artifact, please contact the Director of the Office of University Audits.

#5

Example 2b as it appears in Box:



AUDIT PROCESS

AUDIT OBSERVATIONS

OVERVIEW

The auditor should complete an Audit Observation Form (AO) whenever the auditor identifies a possible (a) opportunity for operational improvement, (b) discrepancy, (c) error, (d) irregularity, (e) weakness or (f) deviation from internal control standards, regulations, or policies. Prior audit reports and linked AOs should be reviewed and used to the extent possible to avoid re-creating an AO already developed.

At the time the auditor identifies an audit concern, they should begin to complete the AO and discuss the observation with the auditee. This discussion should be documented in the applicable fields of the AO. The AO should stand-alone and should document the auditor's analysis (criteria, condition, cause, consequence, and corrective action) related to the finding; this information should not be located elsewhere in the workpapers. The workpaper where the work was performed which resulted in the observation and supporting workpaper references should be DocLinked to the AO in the space provided. Documenting the analysis assists the auditor in preparing to discuss the observation with the auditee.

The AO should document the results of the problem analysis/resolution process. The form is not a step-by-step recipe for doing the work itself, because problem analysis/resolution is not a linear process. Simply completing the form is not a substitute for critical analysis of the situation. The auditor should answer such questions as the following:

- What is the problem that exists?
- How extensive is the problem?
- What is the risk associated with the problem, or lack of controls?
- Do we have our facts correct? Does the auditee agree that the problem exists?
- Are there other controls to compensate for the problem?
- Are there practical solutions to the problem?
- Has management agreed with our recommended corrective action or formulated their own corrective action?

Since the AOs contain the auditor's professional analysis of audit concerns, they are among the most important workpapers created.

ASPECTS OF THE AUDIT OBSERVATION FORM

Other Framework Name: - This dropdown should populated with Risk Ranking
Other Framework Element: - This item indicates the Risk and Priority rating assigned to the AO. Options available to choose from are High, Moderate, and Low. Definitions of the three options are maintained in the Draft Audit Report Template.

FINDING - DESCRIPTION OF OBSERVATION [CONDITION]

This section of the AO should contain a clear and concise statement of the condition. The statement should be concise but provide enough detail to support the reader's understanding of the problem.

Per the IIA Standards, “Condition: The factual evidence that the internal auditor found in the course of the examination (what does exist).”

DISCUSSION AND BACKGROUND - ANALYSIS OF THE AUDIT FINDING [CRITERIA AND CAUSE]

The auditor should document the analysis of the problem in this section. References to applicable standards and/or good business practice should be included. If possible, the auditor should identify probable root causes (as opposed to the symptoms) for the issue.

Per IIA Standards, “Criteria: The standards, measures, or expectations used in making an evaluation and/or verification (what should exist).”

Per IIA Standards, “Cause: The reason for the difference between the expected and actual conditions (why the difference exits).”

RECOMMENDATION [EFFECT AND CORRECTIVE ACTION]

The auditor should include a statement of risk which is sufficient to answer the “so what?” question so that the reason for reporting the observation is clear. This section should also include the corrective action to be presented to the auditee.

This section must be updated to reflect the wording in the External Draft.

Per IIA Standards “Effect: The risk or exposure the organization and/or others encounter because the condition is not consistent with the criteria (the impact of the difference).”

COMMENTS

The auditor should document their discussions of the finding and recommendation with the auditee and other comments as appropriate.

DISPOSITION

The following dispositions are available:

- Mitigating controls - other controls are in place which reduce the risk below the cost of the control.
- Not significant - immaterial error(s) identified.
- Verbal discussion - when the observation is deemed not material for audit report purposes.
- Combined for report - discussed above.
- Not a concern - determined issue was unsubstantiated.
- Future audit concern - outside of the current audit scope.
- Audit report - when the observation is deemed significant and warrants auditor follow-up.
- Observation - pertinent statement of fact that adds context to our report, but for which no recommendation is issued.
- Risk Accepted - management assumes the risk.

The disposition section of the AO form should be updated if the disposition of any AO changes during the report review process.

An AO with an "audit report" disposition should also be DocLinked to the Draft report to provide referenced copies of the report and to ensure AO dispositions accurately reflect the contents of the final report.

For reporting purposes, AOs can be combined for the purposes of clarity or conciseness. When such a combination is appropriate, this should be documented in this field. The auditor should indicate on both the individual observations and the summary/combined observation that concerns were combined for reporting purposes (e.g., different concerns with the same risk). For those documents combined, only the observation used in the report will have a disposition of audit report. Supporting AOs that were combined should have a disposition of "combined for report." Only the recommendation section of the combined form will be updated to reflect the final report language. DocLink's should be created on both the individual AOs and the combined AO for easier review and subsequent follow-up.

An AO may result in more than one recommendation and therefore could be split to provide for two or more distinct implementation dates for follow-up purposes.

Entering an "audit report" disposition causes the following additional fields to appear on the AO:

- **Management Response:** If a written response has been received for AOs that are coded as Audit Report, the response should be scanned and attached to this field.
- **Area Responsible:** This should be the title of the position for which the unit implementing this recommendation ultimately reports (e.g., Chancellor, Provost).
- **Expected Completion:** **<u>This is a very important date</u>**. This is the date that the auditee said they would implement the AO. The first time this field is entered it should be the date agreed to in the audit report. *This date can change if they request a new Expected Completion (EC) date.* When we are provided a new EC date this field changes to the new EC date. The auditor must record this new, extended EC date in this field.

- **Original Expected Implementation Date: <u>This is a very important date</u>**. This is the date that the auditee said they would implement the AO on or before. The first time this field is entered it should be the date agreed to in the audit report. This date should **<u>never</u>** be changed from the date listed in the audit report.
- **Auditor Responsible:** This is the field that notes which auditor is responsible for follow-up.
- **Follow-up Comments:** A field that can be used by the auditor to record general comments but <u>should not</u> be used to document testing. Testing should be placed in the appropriate 1st, 2nd, 3rd or 4th Follow-up Workpapers field.
- **Date Report Published:** Date the report was issued.
- **1st Actual Follow-up Date:** This is the actual date that the auditor did their first follow-up. **2nd Actual Follow-up Date; 3rd Actual Follow-up Date; 4th Actual Follow-up Date** - similar definition applies. <u>Do not</u> fill in this date until follow-up is done.
- **Follow-up Workpapers:** This is the field where the auditor enters their recommendation as to the status (Implemented, In-Progress, Withdrawn, Not Implemented, or New Expected Completion Date). The auditor must also DocLink or type any information relevant to the follow-up recommendation and the work that was performed. This, as noted above, is also the field where the auditor enters the new EC date if a new EC date is given. All follow-up, including changes in the expected completion date, are to be submitted to audit management for approval.
- **Report Item:** This field will be completed by audit management.
- **Set Actual Completion Date:** This field will also be completed audit management.
- **Request review by:** When the auditor has completed any follow-up **1st, 2nd, 3rd or 4th**, select the member of audit management's name in this field to put the work in their review queue. Follow-up must be approved by a member of audit management. Audit Management will not know the auditor has follow-up that needs reviewed and approved unless the auditor sends it to their review queue.

AUDIT PROCESS

AUDITOR TIMEKEEPING

The Office of XXX Audits (Office) maintains records of usage of benefit time in accordance with the XXX System (System) policy. The Office also recordstime spent by audit or project in AutoAudit to assist in reporting audit coverage of System risks, planning of future audits and projects, and evaluating audit staff. Also, at the end of each week, all staff are required to enter time into the AutoAudit time reporting system by phase for planning, fieldwork, and reporting, as applicable to a specific project.

AVSL TIME REPORTING

All audit staff are required to report the use of benefit time monthly in the System Administration Human Resource tool XXX. Recording of benefit time by the staff is performed monthly, by the 16th of every month. The reporting requirements for the various leave categories are available at WWW.XXXX.COM

STATE OFFICIALS AND EMPLOYEES ETHICS ACT REPORTING

The State Officials and Employees Ethics Act (SOEEA) mandates that all Academic Professional and Civil Service employees document all hours worked (twenty-four hours a day, seven days a week) while conducting official System business. Please see the XXX Reporting Policy for Ethics (SOEEA) for further information.

Time spent on System business must be recorded daily to the nearest quarter hour and submitted on a weekly basis (Sunday - Saturday). This may or may not total 40 hours and is to be reflective of actual time spent on System business.

NOTE
Only report time spent on System business on this form; do not report approved leave time (i.e., vacation, sick or other leave time). This information is used to document compliance with the *SOEEA Act* only, and is not used for computation of employees' pay or overtime; or any activities associated with grants and contracts reporting.

See *Time Reporting* in Box (Resources>Red Tab>Administration) for detailed information on auditor time reporting.

REPORTING AND FOLLOW-UP

REPORTING OVERVIEW

REPORTING RESULTS

The report is to include the objective(s) and scope of the audit and an opinion or other applicable conclusion, based upon the audit objective(s) and results of the work performed. The report should also list conclusions, recommendations and action plans, as well as the management and audit team members. Any observations that are significant to communicate to management or background information that would help in readers with the context or risks should be included.

All parties are responsible for adhering to the established reporting format standards. Any proposed revisions to the standard templates are to be discussed among the Directors and approved by the Executive Director. The administrative support staff is responsible for making all formatting changes to the report templates. Consulting reports are not standardized by their ad hoc nature, and as such their unique formats are to be agreed to by audit management in order to meet the needs of the specific engagement.

A copy of the report in PDF format should be distributed as an attachment via e-mail to the individuals on the audit report distribution list. E-mail transmittals for the distribution of audit reports must include the XXX Freedom of Information Act disclaimer. A copy of the audit report, as distributed, should be converted to PDF after the audit is completed and saved in AutoAudit.

REPORT RESPONSIBILITY

The audit report process is as follows:

- The auditor writes the draft report.
- The auditor completes the appropriate sections of the audit report *Checklist*.
- The engagement Director reviews the draft report and the auditor and Director work to resolve any issues or changes.
- A peer review is performed by another member of audit management. If there are no comments, the peer reviewer sends the report directly to the Executive Director for review. If the report has a satisfactory opinion, no Executive Director draft review is necessary
- The Executive Director reviews the draft report and provides feedback. The Executive Director, Director and auditor work to resolve any issues or changes.
- The auditor provides a copy of the draft report to the auditee prior to the exit conference as part of the exit conference notification. An exit conference occurs.
- The auditor and Director make final revisions, if necessary, and concur that the report is ready for publication.
- The auditor obtains approval from the auditee for the final version either via signature on the report or e-mail.

- The Director notifies the administrative support staff that the report is ready for distribution.
- The administrative support staff converts the final version of the audit report to PDF format and develops the report's e-mail transmittal.
- The Executive Director reviews the final report.
- In accordance with IIA Standards, all reports are issued by the Executive Director.

REPORTING AND FOLLOW-UP

EXIT CONFERENCE

PURPOSE

The purpose of an exit conference is to communicate with the auditee the content of the audit 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. Invitees should include the audit participants.

TIMING

The auditor should contact audit participants to determine a suitable time and location for the exit conference and distribution of the draft report. The exit conference should be scheduled as soon as possible while taking into consideration the needs of the auditee. Prior to the exit conference, the draft report is distributed to the planned auditee attendees via e-mail. The template of the draft email distribution for exit conferences is in the Standard Library, Standard Format section of AutoAudit.

DISCUSSION

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 (objective, scope, procedures), what risks we perceived, how we anticipate the recommended action will address the associated risk, and other concerns identified in the audit supported by audit observation forms.

If the auditee is in agreement with the wording and recommendations, the auditor should obtain an expected implementation date and the auditee's signature on the draft report at the exit conference or document agreement in the exit conference minutes. If the auditee is not in agreement with the finding and/or recommendation, 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) per:

- 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 VP (for UA) or Chancellor (for XXX).

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 accepted within the final report.

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.

DRAFT REVISIONS

If significant additional wording changes are needed, a revised draft will be provided to the auditee. Agreement with the revised draft should be obtained prior to issuance and can be evidenced through obtaining a signed report, an e-mail indicating agreement, or by documenting verbal agreement in the work papers.

REPORTING AND FOLLOW-UP

FOLLOW-UP

FOLLOW-UP

Corrective action is subject to follow-up in accordance with the *Standards for the Professional Practice of Internal Auditing* of the IIA.

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:

- 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.
- Withdrawn--the concern no longer exists because of changes in the unit's processes.
- 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).
- Not Implemented--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.

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 considered to be risk-accepted, and will be closed as *Not Implemented*. 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 or risk-accepted the corrective action, the item will be considered to be risk-accepted, and will be closed as *Not Implemented.* 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).

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 –
For all high risk/priority rated corrective action items, in accordance with current policy, the President requires advance approval of any high risk/priority rated recommendations in the draft report where the auditee's proposed expected implementation date exceeds one year, along with the auditee's rationale as to why the implementation is planned to take longer than one year. This information is 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.

Any extensions beyond the original implementation date 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 XXX System (System) VP must meet with the President and the Executive Director of XXX Audits to discuss. At the ABFFC's discretion, the same individuals must also meetwith the ABFFC and the Executive Director of XXX Audits in closed executive session todiscuss. 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* or is risk-accepted and closed as *Not Implemented*.

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 –
Audit evidence in accordance with the *IIA Standards* is to be applied to follow-up work. Internal auditors should ascertain that actions taken on audit findings remedy the underlying conditions.

COMMUNICATION OF FOLLOW-UP RESULTS

Unit –
Follow-up results should be communicated by the auditor to the management team associated with the concern. If the audit concern has been adequately addressed, a verbal or e-mail notification to the unit head is sufficient. If the concern has not been adequately addressed, a

meeting or more formal communication may be required, in accordance with the process described above. Once all recommendations have been closed as either implemented, not implemented, or withdrawn, the auditor should communicate to the auditee, their direct report, and the Executive Director of XXX Audits the closed status of the audit.

XXX Leadership –
On a periodic basis, audit management reports to System management open corrective action items. The decision of which action items to report is based upon input from the Audit, Budget, Finance, and Facilities Committee and the President. On a quarterly basis, the Executive Director reports to the President and the Audit, Budget, Finance, and Facilities Committee all high and moderate risk/priority rated corrective action items that have been risk-accepted by management during that quarter.

Board Reporting –
Statistics of the follow-up process for all XXX audits are provided to the Board in the Annual Report.

REPORTING AND FOLLOW-UP

ANNUAL REPORT

PURPOSE

The purpose of the Annual Report is to describe our service to the XXX 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 Reportalso satisfies the Fiscal Control and Internal Auditing Act 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.
This Report is also provided as a written document to the BOD by September 30th. To protect the Office's FOIA exemption, communication of significant findings is highly summarized in the publically available Annual Report, and is provided in more detail through the Audit, Budget, Finance and Facilities Committee (ABFFC) presentation and quarterly reporting to the President and ABFFC.

PERSONNEL

PERFORMANCE APPRAISAL PROCESS

OVERVIEW

The Office adheres to the XXX System Performance Appraisal Process. Performance appraisals provide employees with a clear understanding of their goals, areas in which they have excelled, and areas which are in need of more focus. Performance feedback occurs on various levels: continual feedback, the annual performance appraisal process, and anoptional mid-year review of employee goals.

Continual feedback is provided on an informal, continual basis throughout the year. Performance appraisals as a part of a continual process of communication and coaching are a valuable tool that allows supervisors and employees to check-in and see how they are doing. Continual performance feedback is a key to motivating employees and reaching organizational goals.

The annual performance appraisal process utilizes several tools, some of which are required by our Office policy while others are optional. The Executive Director or Director (supervisor) initiates the annual performance appraisal process.

Additionally, the supervisor and employee may meet on a semi-annual basis to review employee goals. The supervisor schedules and facilitates the meeting to discuss progress toward meeting the current year's goals.

The Performance Appraisal Forms are available from the Human Resources Website at https://hrnet.uihr.uXXX.edu/UHR/PerformanceAppraisal/index.cfm (this site requires Enterprise Authentication Login).

REQUIRED ANNUAL PERFORMANCE APPRAISAL FORMS

Employee Goals – Divided into three segments of previous year's goals, next year's goals, and professional development goals.

Performance Assessment – Based on competencies identified as key factors for successful performance. Provides areas for describing how an employee has demonstrated the competencies, and / or identifying areas that could be further developed.

OPTIONAL ANNUAL PERFORMANCE APPRAISAL FORMS

Optional Employee Worksheet – This form provides an opportunity for employees to provide input into the annual assessment and includes sections for any special contributions that the employee would like considered.

PERSONNEL

TRAINING AND PROFESSIONAL DEVELOPMENT

GENERAL

Each auditor should possess a body of specialized knowledge and should maintain a recognized, continuous process of education in order to sustain continuous professional growth in the field of Internal Auditing. Below are the CPE requirements of the State Internal Audit Advisory Board (SIAAB), Certified Internal Auditors (CIA), Certified Information Systems Auditors (CISA), and Certified Fraud Auditors (CFE).

STATE INTERNAL AUDIT ADVISORY BOARD REQUIREMENTS

In compliance with the requirements established by the State of XXX Internal Audit Advisory Board's *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 XXX System (System) operates.

The 80 hours of CPE must be satisfied during two successive (non-rolling) calendar years such as 2016-2017 or 2018-2019. 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.

Auditors required to take the total 80 hours of CPE should complete at least 20 hours of CPE in each year of the 2-year period. The 20-hour minimum for each CPE year would not apply when a prorated number of hours are being used to cover a partial 2-year CPE period. It is the Office of XXX Audits' (Office) 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.

For additional information on CIA requirements go to the IIA website:
https://na.theiia.org/certification/cia-certification/Pages/CPE-Requirements.aspx
https://na.theiia.org/certification/Public%20Documents/Administrative-Directive-No-4.pdf

CISA REQUIREMENTS

The CISA continuing professional education policy requires the attainment of continuing professional education hours over an annual and three-year certification period. CISAs must comply with the following requirements to retain certification:

- Attain and report an annual minimum of 20 continuing professional education hours.
- Submit annual continuing professional education maintenance fees to ISACA international headquarters in full.
- Attain and report a minimum of 120 continuing professional education hours for a three-year reporting period.
- Respond and submit required documentation of continuing professional education activities if selected for the annual audit.
- Comply with ISACA Code of Professional Ethics.

The annual reporting period begins on January 1 of each year. The three-year certification period varies and is indicated on each annual invoice and on the letter confirming annual compliance.

For additional information on CISA requirements go to the ISACA website:

http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Pages/Maintain-Your-CISA.aspx

CFE REQUIREMENTS

The minimum CPE required is 20 hours per calendar year of which at least 10 hours must relate directly to the detection and deterrence of fraud. CPE hours in excess of the minimum requirements may carry forward 10 extra hours to meet the requirements of future years.

For additional information on CFE requirements go to the Association of Certified Fraud Examiners website:

http://www.acfe.com/cpe-index.aspx

CPE RECORDS

Auditors are responsible for recording their CPE activity in Auto Audit. This includes adding any new certifications received and attaching any applicable backup documentation. CPE sponsored by the Office will be entered in Auto Audit by the Officeprior to distribution of the certificate.

Each auditor should retain a letter, certificate, or other written independent attestation of completion of all coursework. Also, documentation supporting the content and location of the seminar, meeting, etc. (other than training presented by the Office) should be retained by each auditor.

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

TUITION WAIVERS

Subject to System rules and regulations, staff members may receive tuition waivers for System courses. Released time may be granted for job-related courses, subject to the needs of the department, in accordance with the System rules and regulations. Staff members are encouraged to participate in advanced degree programs that will assist in the career advancement goals. Attendance at on-campus job-related training sessions given by campus units (such as nonacademic classes and computer and accounting classroom sessions) as well as off-campus seminars, conferences, and training sessions are encouraged. All of these educational activities require the approval of audit management if the hours involved are during regular working hours. 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, System courses, other XXX or college courses, professional society courses, or specialized review courses. Released time may be granted in accordance with the preceding paragraph. 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 Office 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.

APPROVAL REQUIRED

Funding for courses, training, and memberships is subject to budgetary constraints.

All specific training, in whatever mode, will be subject to System and Office production schedules and needs for audit personnel support. Management approval is required prior to registering for a training event.

PERSONNEL

EMPLOYEE ORIENTATION

Upon hiring a new employee, a New Employee Checklist and Orientation will be Completed. An orientation program provides each new employee with information regarding the Office of XXX Audits and the XXX System as a whole.

To announce the hiring to the staff, an e-mail will be distributed by audit management introducing the new employee and providing some educational and work experience background.

The template for the New Employee Checklist and Orientation is in \\ui\audits\resources\Forms\.

PERSONNEL

PESONNEL MANAGEMENT

STANDARD WORKDAY

The standard workday is 8 hours for academic professional staff and 7.5 hours for civil service staff.

FLEX TIME

The personnel policies of the XXX System (System) provide for the possibilityof the use of flex time. A staff member who desires to work a flex-time schedule should provide a proposed written schedule to audit management. Audit management must approve the flex-time schedule. Requests will be granted based upon the collective best interest of the employee and the Office of XXX Audits (Office).

When the needs of the department or a specific audit that an individual is working on requires a modification from the adapted flex-time schedule, it is expected that the staff member will make the necessary adjustments as required.

ELECTRONIC CALENDAR MAINTENANCE

Each staff member is to update the electronic calendar to reflect time away from the office for fieldwork or appointments. The calendar should contain location information for emergency purposes and should also reflect free and/or busy periods to facilitate scheduling.

ABSENTEEISM

Those individuals absent due to sickness or other reasons not approved in advance (Out of Office Request) should notify audit management as soon as possible and explain the reason. Notify the Office daily with an update of your condition.

JURY DUTY

Staff members called for jury duty are required to provide a copy of the jury duty summons to audit management, prior to appearing for jury duty.

VACATION TIME

Requests for vacation leave will be granted with due regard for the operating needs of the Office. Management is responsible for vacation scheduling within the Office that will best meet and reconcile Office work requirements with vacation preferences of employees. Requests for

more than a day or two should be scheduled well in advance. Under hazardous weather conditions, an employee may leave at their own discretion when concerned about personal safety, but time away from the office must be charged against vacation time.

HOLIDAYS

Holiday policy will be observed in accordance with the respective individual campus policies. Any questions should be addressed with audit management.

Current holiday schedules for all three campuses can be found from the Human Resources website at: https://www.hr.uXXX.edu/leave/holidays

FLOATING HOLIDAYS

General

- Floating holiday(s) **must be taken between July 1 and June 30**; unused floating holiday(s) leave will not be carried forward to the next fiscal year. A staff member who separates employment with the XXX and who has not taken his/her floating holiday before the date of separation will not be compensated for that day.
- **A floating holiday must be taken in full at one time.** For part time staff members between 50% and 99% of full time service, the floating holiday must be prorated.

OTHER TIME OFF AND LEAVE INFORMATION

Other System Policy time off and leave information can be found from the Human Resources website at: https://www.hr.uXXX.edu/leave

ADMINISTRATIVE PROCEDURES

COMPUTERS

INFORMATION SECURITY

Data Ownership: All data kept on the Office of XXX Audits' (Office) network should pertain to the XXX System and related professional duties of the audit staff. Assuch, these files are considered the property of the Office, rather than the property of the individual who has created them.

ACCEPTABLE USE OF COMPUTING AND NETWORK RESOURCES

System Offices employees must comply with the guidelines outlined in this policy. It is the employee's responsibility to thoroughly review this policy and it 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. AutoAudit and Lotus Notes issues, contact the Director of IT Audits

2. All other computer, application, or network issues and problems need to be reported directly to the Microcomputer Support Specialist (MSS).

    a. The MSS will notify the user how the issue will be handled, e.g., the MSS will attempt to resolve the issue or will identify who the issue/problem was passed to or will notify if the user needs to resolve the issue.
    b. The MSS will address the situation first, attempting to handle workstation and local server issues. If the MSS cannot solve the issue quickly, the computer will be replaced with the office backup computer. The MSS will then work on the problem computer on an ASAP basis in conjunction with other responsibilities.
    c. If the MSS cannot solve the problem, is unavailable, or if the problem is not a workstation issue, contact the Director of IT Audits.
    d. If the issue cannot be solved by local resources or those resources are unavailable, please review the service solution options at https://www.aits.uXXX.edu/get_help.

LAPTOP COMPUTERS

Laptops assigned to staff are the responsibility of the staff person until returned. Staff members who have a laptop assigned to them should not loan that laptop to other staff members, family members, or friends.

The following procedures should be followed when using and storing laptop computers.

Laptop Care

1. Laptops should be transported in their protective carrying cases at all times.
2. Laptops should be protected from temperature extremes and precipitation (rain, snow, sleet, and ice).
3. Staff members should refrain from placing drinks or food near laptops and in places where spills could cause damage to the laptop.
4. The laptops are provided with all the necessary software. **Do not download any software to the laptop, or install any software to the laptop without the approval of the Microcomputer Support Specialist.**

Laptop Security – In the Office

1. Doors to offices with laptops should be locked over the lunch hours.

2. A designated staff person will be responsible for the safeguarding of, and accountability for, any laptops not assigned to a particular staff member.

Laptop Security while out of the Staff Member's Home Office

1. Laptops should be either secured during lunch or any other time the auditor is away from his working area (e.g., while interviewing auditees or touring facilities).

2. Preferably, laptops should not be left unattended in automobiles. However, if it is necessary to leave the laptop in an unattended car for a short period of time, the laptop should be placed in the trunk.

ADMINISTRATIVE PROCEDURES

RECORDS RETENTION POLICIES

RECORDS DISPOSITION AUTHORIZATION

A Records Disposition Authorization, Application #UI-01-10, for the Office of XXX Audits (Office) 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 Office to dispose of, or transfer to the State Records Commission/ Archives, the records as 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. On an annual basis, audit reports that have reached the 20-year retention period are forwarded to the XXX Archivist (Archivist) in a non-proprietary format such as PDF. Audit management must ensure all recommendations have been closed, and no litigation is pending or anticipated in regard to the related audits or audited units prior to transfer to the Archivist. Such audit reports may then be disposed of in accordance with the Records Disposal section below.

WORKPAPER FILES – FISCAL YEARS 1996-PRESENT

All audit work papers are retained for a period of 10 years from audit completion (report issuance). Work papers are retained in electronic format. Backup (redundant) copies of all work paper 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, provided that audit management has ensured all recommendations have been closed, and no litigation is pending or anticipated in regard to the related audits or audited units.

GENERAL CORRESPONDENCE FILES

General correspondence files include final, formal correspondence outside of the AutoAudit process such as routine correspondence, copies of XXX System reports generated by other offices, and memoranda relating to XXX 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 Office is considered to be historical record. On an annual basis, historical records that have reached the 5-year retention period are forwarded to the Archivist. Generally,

such historical record includes correspondence from the Executive Director of XXX Audits.

OTHER RECORDS

Other Office records are to be retained in accordance with the OBFS Policies and Procedures Manual.

RECORDS DISPOSAL

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

References:

- OBFS Section 1.4 – XXX Business & Financial Records Management: https://www.obfs.uXXX.edu/bfpp/section-1-intro-business-financial-functions/business-financial-records-management
- Records and Information Management Services: https://www.uXXX.edu/cio/services/rims/retention_and_disposal/records_disposal/
- RIMS Disposal Flowchart: https://uofi.app.box.com/s/4z46vauxuexwxerwqukc1edwu80mhhak

ADMINISTRATIVE PROCEDURES

GENERAL POLICIES

OFFICE POLICY AND PROCEDURES RELATED TO POSSIBLE FRAUD OR CRIMINAL ACTIVITY

If you suspect or are provided information regarding potential criminal activity, inform audit management. Initiation of any response to a potential fraudulent or criminal activity is to be handled by audit management.

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. 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

The following information is intended to serve as a common sense guide to appropriate attire for all Office of XXX Audits employees during the core business hours of 8:00 a.m. – 5:00 p.m. Staff will be expected to dress in a manner appropriate to their business activities and schedule on each particular day.

When working at an auditee site or meeting with an auditee, auditors should be dressed in either business or business casual attire that conforms to the auditee's dress code. Meetings with Directors and above and opening and exit conferences normally require regular business attire (i.e., suits or sport coats with dress slacks and dress shirts with ties are appropriate for men. Suits, dresses, or skirts or slacks with coordinating jackets are acceptable for women.). Check with audit management if you have a question.

Business casual attire is acceptable at all training sessions sponsored internally or externally unless notified otherwise.

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 (e.g., clothing more appropriate to yard work, exercise class, picnic, playing sports, or night-clubs). Again, check with audit management if you have a question.

Regardless of dress style, all clothing should be neat, clean, pressed, and without holes or ragged edges.

Examples of Acceptable and Unacceptable Casual Dress

Listed below is a general overview of acceptable comfortable casual wear as well as a listing of some of the more common items that are not appropriate for the office. Neither group is intended to be all-inclusive. Rather, these items should help set the general parameters for proper casual wear and allow you to make intelligent judgments about items that are not specifically addressed. A good rule of thumb is if you are not sure if something is acceptable, choose something else or inquire first.

Item	Acceptable	Unacceptable
Pants	Clean, wrinkle-free cotton pants (khakis, cargo pants), capri or gaucho pants (below the knee level), or jeans.	Sweatpants, wind suits, shorts, leggings, spandex.
Shirts	Casual shirts, golf shirts, sweaters, turtlenecks.	Tank tops; shirts or other clothing items (e.g. caps) with profanity or offensive slogans; halter tops; t-shirts (unless worn under another shirt, blouse, dress, etc.).

Item	Acceptable	Unacceptable
Dresses & Skirts	Casual dresses, skirts, and split skirts at or below knee level.	Mini/micro-skirts; spaghetti-strap dresses.
Footwear	Loafers; clean athletic shoes; boots, flats; dress sandals or open-toed shoes; clogs; leather deck shoes (hosiery/socks are optional if appropriate with the remainder of the outfit).	Flip-flops; slippers.

If an item of clothing is deemed to be inappropriate by the employee's supervisor, the employee will be sent home to select more appropriate clothing before returning to the office.

Exceptions

As with any policy, there are exceptions. Alternative attire will be appropriate for certain audit activities (i.e., farm audits, taking physical inventories). Audit management will determine whether any special events or tasks require alternative attire.

APPENDIX A

OFFICE OF XXX AUDITS WORKPAPER GUIDELINES

At a minimum, workpapers must document relevant information to support the conclusions and engagement results. Among other things, workpapers may include:

- Planning documents and audit procedures.
- Control questionnaires, flowcharts, checklists, and narratives.
- Notes and minutes resulting from interviews.
- Organizational data, such as charts and job descriptions.
- Copies of important documents.
- Information about operating and financial policies.
- Results of control evaluations.
- Letters of confirmation and representation.
- Analysis and test of transactions, processes, and account balances.
- Results of analytical review procedures.
- Audit reports and management responses.
- Audit correspondence that documents the audit conclusions reached.

Scanned Documents –

Scanned documents should include a reference to the source and the purpose of the document when relevant to understanding or appreciating the actual audit work performed. Such information needs to be included only when it is not provided elsewhere in the workpapers or apparent by the actual document.

Web Intelligence (Webi) –

Webi is a frequently used tool for generating and analyzing data. In order to preserve the readability and access of audit work, such work must be saved to Excel and included in the workpapers for all investigations. Conversion in other projects is encouraged.

Weblinks –

When using references to websites in audit workpapers, to help ensure the site can be readily accessed in the future, both the name of the site and a hotlink to the website should be included. If specific information from a website was referenced (e.g., Federal Register, IRS publications, various guidelines), the webpage should be saved to a file and attached to the workpapers.

Tick marks –

Tick marks do not need to be standardized throughout the set of workpapers, but must be consistent throughout a particular workpaper. Tick mark explanations must be a part of the workpaper.

Doclinks (cross-referencing) –

Workpapers should be prepared using the appropriate DocLinks (cross-referencing). A DocLink from the Audit Procedures to the primary workpaper provides a reference to where the work was performed. It is not necessary to DocLink all workpapers to the Audit Procedures - only the primary workpaper. The primary workpaper will then contain DocLinks to other, supporting workpapers, which provide additional information regarding the audit procedures performed, results, conclusions reached, and audit observations.

DocLinks should be used to reference information useful in more than one place or to other relevant information including the source of information, composition of summary totals, or other documents or examples of transactions. Documents/information should be in the workpapers only once.

APPENDIX B

There are eighteen different types of personal identifiers that should be segregated. They are:

1. Names
2. Geographic subdivisions smaller than a State, including:
    a. Street address
    b. City
    c. County
    d. Precinct
    e. Zip codes and their equivalent geocodes
3. Telephone numbers
4. Fax numbers
5. E-mail addresses
6. Social Security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. All elements of dates (except year) for dates related to an individual, including:
    a. Birth date
    b. Admission date
    c. Discharge date
    d. Date of death
    e. All ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
11. Certificate/license number
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable image
18. Any other unique identifying numbers, characteristics, or codes