



UW INSTITUTIONAL AUDIT MANUAL

July 2010

Audit Manual

Table of Contents

- Chapter 1 Introduction
 - Audit Manual Purpose
 - Audit Manual Organization
 - Role of Internal Audit
 - Types of Audits and Engagements
 - Auditor Ethics
 - Audit Resources
 - Continuing Education

- Chapter 2 General Audit Administration
 - Management of Working Papers
 - Quality of Working Papers
 - Supervision of Staff

- Chapter 3 Audit Planning
 - Annual Audit Plan
 - Individual Audit Strategy
 - Review of Internal Control Environment
 - Entrance Conference

- Chapter 4 Audit Evidence
 - Standards of Evidence
 - Types of Evidence
 - Types of Audit Procedures

- Chapter 5 Concluding the Audit
 - Evaluating Audit Issues and Tracking Findings
 - Exit Conference
 - Communicating Audit Findings

- Chapter 6 Investigative Audits

- Appendix A: UW System and Higher Education Key Terms, Acronyms, and Definitions

CHAPTER I

Introduction

This Audit Manual is a reference document for the UW institutional and System Administration auditors. The manual covers the expectations and procedures that apply to our audit work in many areas: general audit administration, audit planning, audit evidence, and concluding the audit. The manual also includes an appendix of commonly used terms, acronyms, and definitions.

Audit Manual Purpose

The Audit Manual documents the auditing policies and procedures of the UW institutional and System Administration auditors. The policies and procedures are intended to ensure the quality of all audits and other engagements and to ensure consistent and efficient audit procedures.

This Audit Manual also serves as a training aid for new employees. The standard procedures and suggested methods in the manual should provide guidance for our audits. More experienced staff should use the Audit Manual as a reference guide for current auditing procedures. All professional UW System audit staff are expected to keep up-to-date on the guidance and procedures described in the manual and apply them, when practical, in their audit work.

This manual is not intended to restrict independent thinking or innovative approaches to auditing. Auditors should continue to use judgment while planning and conducting audits. As needed, the policies and procedures described in this manual may be modified as necessary to fit the special circumstances of the audit. Auditors should use their experience, auditing skills, and judgment to determine when it is necessary to modify the procedures included in the manual.

Audit Manual Organization

Amendments to the manual will be made when warranted. Significant additions, deletions, or amendments to the manual will be discussed with the UW System internal auditors. Each UW auditor is encouraged to submit recommendations for additions, deletions, or amendments to the Audit Manual through the Director of the UW System Administration Office of Operations Review and Audit.

Role of Internal Audit

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps UW System management and the Board of Regents accomplish their objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The specific mission statements or charters for internal audit functions may vary by UW System institution and can be obtained from the individual institutions. However, in general, all institutional auditors should ensure the reliability and integrity of internal controls and information, as well as provide support to members of the University in the effective discharge of their responsibilities. To this end, internal auditors will furnish their institutions with objective analyses, recommendations, counsel, and information concerning the activities examined.

As provided for in the institutional audit charters, UW System internal auditors have the authority to audit all parts of their respective institution and have full and complete access to any of their institution's records, physical properties, and personnel relevant to the performance of an audit. Documents and information given to internal auditors during a review or audit will be handled in the same prudent manner as by those employees normally accountable for the information.

Internal auditors have no direct responsibility or authority for any of the activities or operations they review. They should not install procedures, prepare records, or engage in activities that would normally be reviewed by internal auditors.

Internal auditors may serve as the liaison with external auditors, including those from the UW System Administration Office of Operations Review and Audit, the Legislative Audit Bureau, and various federal agencies. When this is the case, the internal auditor will ensure appropriate institutional staff are aware of the audit, its objectives, external auditor needs or requests, and audit findings. The internal auditor may also be responsible for coordinating the institution's response to draft reports or findings.

Types of Audits and Engagements

UW institutional and System Administration auditors conduct a variety of audits or projects, including:

- **Financial and compliance audits** determine whether financial operations are properly conducted, whether the UW accounting systems and internal controls are adequate, whether the financial statements are presented fairly, and whether the UW institution has complied with applicable laws, regulations, and provisions of contracts and grant agreements.
- **Attestation and/or other financial-related engagements** concern examining, reviewing, or performing agreed-upon procedures on a subject matter or an assertion about a subject matter and reporting on the results.

- **Investigative audits** are designed to verify the existence and magnitude of suspected fraud, abuse, and financial irregularities. The internal auditor should utilize the highest level of discretion when undertaking such an audit. He or she should promptly notify the UW System Administration Office of Operations Review and Audit and any members of institutional management deemed appropriate.
- **Management audits** determine whether the UW institution is managing its resources in an economical, efficient, and effective manner.
- **Information technology (IT) audits** determine whether the UW institution's IT environment supports the business objectives and whether undesired events are prevented or detected and corrected.
- **Program evaluation audits** determine whether the desired results or benefits of a UW program are being achieved and whether program objectives established by the Board of Regents, Wisconsin State Legislature, UW System Administration, Chancellor, or other authorizing body are being met.
- **Consulting projects** may range from formal engagements, defined by written agreements, to advisory activities, such as participating in standing or temporary management committees or project teams.

Auditor Ethics

To be effective in performing audits, UW System internal auditors must be independent and objective, both in actuality and perception. UW System employees, including institutional and System Administration auditors, are bound by certain ethical rules that apply to all state employees.

The Code of Ethics for unclassified staff is detailed in Wisconsin Administrative Code UWS 8. Wisconsin Administrative Code ER-MRS 24 provides the Code of Ethics for classified staff. In general, unclassified and classified staff, including internal auditors, should not accept anything of value from an employee, supplier, or business associate of the University which would impair or be perceived to impair their professional judgment or objectivity.

Audit Resources

Many resources are available to assist UW System internal auditors to conduct audits and develop their skills. This manual is intended to provide general guidance and to refer auditors to other resources, where appropriate.

Each UW System internal auditor benefits from maintaining a set of reference materials and becoming familiar with the types of resources available. Auditors may have their own

personal electronic or paper copy of some resources while other reference materials are available on the internet, such as:

- UW System Financial and Administrative Policies (<http://www.uwsa.edu/fadmin/fap.htm>);
- UW System Board of Regents' Regent Policy Documents (<http://www.uwsa.edu/bor/policies/rpd/>);
- Wisconsin Statutes and Administrative Code;
- University of Wisconsin System Fiscal and Accounting General Records Schedule (<http://www.uwsa.edu/gc-off/records/schedules/>);
- IIA Auditing Standards (<http://www.theiia.org/guidance/standards-and-guidance/>);
- ACUA benchmarking survey, control assessment tool, and risk dictionary – password required (<http://www.acua.org/>);
- AICPA Auditing Standards;
- AICPA Audit Guide: *Audits of State and Local Governments*;
- AICPA Audit Guide: *Government Auditing Standards and Circular A-133 Audits*;
- other AICPA audit guides and AICPA self-studies;
- GASB statements, codification, interpretations, technical bulletins, implementation guides;
- *Journal of Accountancy* and *CPA Journal*;
- ISACA and ITGI's *Control Objectives for Information and Related Technology* (COBIT) (<http://www.isaca.org>);
- Department of Administration's State Accounting Manual;
- Department of Administration's GAAP Conversion Policies and Procedures Manual;
- OMB Circular A-133 (Audits of States, Local Governments, and Non-Profit Organizations);
- OMB Circular A-133 Compliance Supplement;
- OMB Circulars A-21, A-87, and A-110;
- Catalog of Federal Domestic Assistance;
- Code of Federal Regulations (<http://www.gpoaccess.gov/fr/>); and
- Accounting, auditing, and/or IT textbooks.

In addition, the UW System internal auditors have created a mechanism known as PantherFiles to share files, such as audit programs and reports, across UW institutions. To obtain access to PantherFiles, please contact the UW System Administration Office of Operations Review and Audit.

Continuing Education

As professionals, UW internal auditors must demonstrate proficiency in terms of the key knowledge, skills, and abilities required to effectively conduct internal audit assurance engagements. In addition, they must stay abreast of recent developments in their profession. Therefore, each UW internal auditor is encouraged to sustain continuous

professional growth in the field of internal auditing through training, certification, and participation in professional organizations.

Each UW internal auditor should consult with his/her supervisor regarding funds available for continuing education and the amount of time that will be devoted to such activities. If continuing education credits will be used for certification or professional membership purposes, the internal auditor should also maintain documentation of his/her continuing education.

CHAPTER II

General Audit Administration

Maintaining audit documentation, ensuring the quality and integrity of that documentation, and supervising staff (where applicable) are necessary to fulfill audit responsibilities and ensure that audit work is adequately supported. Working papers are essential to this objective as they both support auditor's findings, conclusions, and recommendations and assist in managing the audit work.

Management of Working Papers

The term "working papers" includes all hard-copy and electronic documents collected or prepared during a given audit. In the performance of audit work, the Standards for the Professional Practice of Internal Auditing state that "Internal auditors should collect, analyze, interpret, and document information to support audit results." The internal auditor's working papers will provide the principal evidence that these standards were met and the audit was performed professionally.

Working papers provide the basis and support for the conclusions reached by the internal auditor. All relevant working papers prepared during an audit will be preserved and included in the UW-maintained files. UW System internal auditors should take steps to protect the integrity of the working papers, ensure working papers are available for inspection during the period of time they must be maintained, and limit access to avoid unauthorized loss of information or compromise confidential information contained in the working papers.

Indexing

Working papers should be indexed in some manner to ensure auditors, UW management, and others are able to easily understand how the audit program links to the working papers or audit evidence and how the working papers link to the final communication with the auditee. Index or summary sheets will list the index number, working paper name, and preparer's initials and date. It is recommended that UW System internal auditors index working papers as soon as they are completed to safeguard against loss and facilitate cross-referencing. The specific indexing system may vary by audit and by UW institution.

Protection and Confidentiality of Information

It is the responsibility of every UW System internal auditor to understand the security requirements related to their audit and collected information and to meet those requirements, including security needs of physical working papers, electronic files, materials, and equipment. In general, UW auditors are responsible for the safe custody of paper and electronic working papers, as well as UW institutional information they have obtained during the course of the audit.

Working papers may contain sensitive, confidential, or personal information, such as that contained in employee personnel files, which by law or regulation may not be available to the public. Working papers may also contain information that indicates the presence of fraud or illegal acts. Working papers may or may not be legally confidential. Therefore, open records requests for working papers should be forwarded to the institutional public records custodian.

Physical Records

To protect confidential UW information, as well as to protect *preliminary* results and conclusions reached during the audit, working papers should not generally be left out in the open where they might be accessible to the public or other UW personnel.

UW System internal auditors should take additional steps when working with physical records that are protected by the primary record owner. Any record that is considered confidential while in the primary record owner's possession should also be kept confidential by the auditor.

Working papers that include protected information should be designated by writing "CONFIDENTIAL" at the top of that working paper, as well as indicating this on the index or summary sheet, in case the working paper needs to be redacted before being reviewed by an outside party. Protected working papers may be stored separately from the audit file in a secure manner, such as a locked cabinet in the UW auditor's office or in electronic files with restrictive access controls.

Electronic Records

To avoid inadvertent loss or theft of electronic data, including information that may be confidential, it is the UW System internal auditors' policy that electronic audit files must be stored in a location that meets security needs. At times, internal auditors may need to use portable means of data storage, such as flash drives, laptops, and disks. Internal auditors should avoid, where possible, storing permanent audit files on portable media, unless there are extenuating circumstances and they are promptly removed when such storage is no longer necessary. Internal auditors should also avoid storing audit documentation on network drives that are shared with other offices or non-audit staff. Finally, to protect information it is important that computers are physically secured at all time and unattended terminals are locked.

Retention

When working papers are no longer needed for reference, they should be boxed, labeled, and sent to the State Records Center or campus archive location. In accordance with the UW System Fiscal and Accounting General Records Schedule, the standard retention period for financial audit files, reports, and findings is 10 years or until the date of the next audit, whichever comes first.

Quality of Working Papers

As it relates to working papers, quality means that the audit objectives are met, efficient and defensible techniques are used, the working papers comply with the auditing standards (if applicable), and evidence in the working papers is persuasive enough to convince an experienced auditor of the soundness of the opinions and conclusions. An independent reviewer should come to the same conclusion as the preparer given the findings and analyses documented in the working papers.

All working papers prepared by UW System internal auditors should be prepared in good form with proper attention to layout and legibility, with complete headings, explanations of sources, and verification of work performed. The internal auditor should generally observe the following rules when preparing working papers:

- Every working paper will be properly identified. The working paper will include the name of the auditee, a description of the information presented, and the period covered or applicable date.
- Working papers will be understandable without detailed supplementary oral explanations. Working papers will also be complete and concise.
- Working papers will be linked or cross-referenced to the audit program.
- The source of the data presented on each working paper will be clearly stated.
- The nature of verification work performed by the internal auditor will be indicated in each working paper. A review of paid invoices, for example, might be supplemented by the testing of related purchase orders to substantiate the authenticity of the invoices examined; a description of this verification procedure would be included in the working papers.
- The use of audit tick mark symbols may aid in identifying the procedures followed in conducting an audit test and avoiding lengthy explanations. Whenever symbols are employed, they will be accompanied by a legend explaining their significance.
- The extent and scope of sampling will be clearly stated at every phase of the audit to which it is applied; accordingly, the working papers will disclose the character and extent of all sampling methods utilized.

Supervision of Staff

UW System Administration, UW-Madison, and UW-Milwaukee have internal audit offices with multiple auditors and analysts. While UW comprehensive institutions generally have one full-time auditor, they may employ student interns or employees to assist in accomplishing their audit objectives. In all cases, the audit supervisors should communicate to staff auditors all matters relevant to their assignment(s) that might affect the nature, timing, and extent of audit procedures necessary to meet their audit objectives. Staff auditors should periodically communicate their progress, findings, and difficulties to their supervisor to determine the potential effect on the audit.

The audit supervisor has both the responsibility and the authority to take steps to ensure staff auditors understand and are working to achieve the desired audit results. To ensure

this is accomplished, audit working papers should be periodically reviewed by the supervisor. This review should be documented in some manner. The supervisor also has the duty to correct any activities or behavior detrimental to the audit effort or to the professionalism expected from UW System internal audit staff.

CHAPTER III

Audit Planning

The assessment of audit risk is an integral part of the planning process. The audit planning process encompasses all activities related to the development of the internal audit plan and individual audit strategy, which should include the determination of the audit scope and objectives. The primary objective of the audit planning process is to design an audit approach that helps ensure audits achieve their objective(s) and are performed in the most effective and efficient manner.

Annual Audit Plan

Determining which UW entities or functions to audit is a continuous and complex process. Given the number of internal auditors per UW System institution and the large number of operating units and functions within each institution, it is important to primarily allocate audit resources to high risk exposures. Therefore, each UW System internal auditor or internal audit office will annually define the potential audit universe at their UW institution, perform an analysis in order to assess risks, and schedule audits based on the priorities established and level and expertise of the internal auditor(s).

The risk analysis will combine factual information and internal auditor judgment in the selection, ranking, and weighing of the various audit risk factors. Financial, compliance, operational, reputational, strategic, IT, and safety risks may all be considered in the analysis. When conducting a risk assessment, internal auditors should communicate with and obtain the opinions of institutional management and staff. Other key sources of information will vary but may include the institution's internal control plan; UW System Administration staff; federal and state laws/regulations; previous internal and external audit reports and working papers; appropriate articles, papers, and studies that outline current trends or threats and their impact on the risk areas; and other UW System audit staff who have been involved in similar audits or are familiar with the subject matter.

It should be emphasized that the final determination as to which areas should be included in the audit plan cannot be based solely on the results of this audit risk assessment. Rather, the performance of the assessment is a tool for use by internal auditors. In addition, the annual audit plan must remain flexible to accommodate unanticipated but high priority audits, which may include potential fraud reviews or requests from senior management.

The annual audit plan should be reviewed and approved by appropriate members of institutional management, which may vary by institution.

Individual Audit Strategy

At the outset of the planning phase, an audit is usually defined in very broad terms. Once an audit has been identified in the audit plan, the auditor must establish and finalize the

specific scope and objectives. The auditor must identify the risks associated with the audited entity. In so doing, the auditor should ensure that audit resources and effort are devoted to the key areas that can have a significant impact on the performance and results of the function, program, or activity being audited. The auditor should also determine the time period being reviewed, which may be one or multiple years; timing of the audit, such as one year after implementation of a new system or procedure; design of detailed procedures, including audit criteria and methodology used; and anticipated reporting. At the end of the planning phase, the internal auditor should be able to clearly articulate what will be audited, why it will be audited, and how it will be audited.

The planning conducted by UW System internal auditors should be documented and should include:

- establishing audit objectives and scope of work;
- obtaining background information about the activities being audited;
- determining the resources necessary to perform the audit;
- communicating with all who need to know about the upcoming audit;
- as appropriate, becoming familiar with the activities and controls to be audited, to identify areas of audit emphasis;
- writing the detailed audit program; and
- determining how, when, and to whom audit results will be communicated.

The audit strategy developed in preliminary planning is intended to be reevaluated during the course of the audit. Subsequent changes to the audit strategy and the effect on the audit should be added to the working papers as appropriate. Issues to consider in modifying the strategy include, but are not limited to: fraud or red flags of fraud being encountered during the audit; significant delays in receiving or changes in the availability of audit evidence; major changes in the organization (e.g., key staff or restructuring); and subsequent decisions by the auditee (e.g., change in accounting policy).

Review of Internal Control Environment

An internal control is any action taken by management or staff to enhance the likelihood that established goals and objectives will be achieved, while mitigating risks and protecting assets, including money, reputation, physical property, and human resources. UW System internal auditors need to develop a sound understanding of the function, program, activity, department, or unit being audited, including policies and internal controls over business processes and the systems used to support these business processes. This understanding will assist in designing and performing audit procedures.

The internal control environment may address a variety of objectives for the auditee, while the auditor may be primarily interested in only certain ones, such as the controls to help ensure accurate financial statements or those to address significant compliance requirements. Ultimately, UW System internal auditors should use judgment in identifying internal control processes that are relevant to the audit in question.

Components of internal control include:

- Control environment – This incorporates the entity’s overall tone and typically includes the following elements: communication and enforcement of integrity and ethical values, commitment to competence, participation of those charged with governance, management’s philosophy and operating style, organizational structure, assignment of authority and responsibility, and human resource policies and practices.
- Risk assessment – This includes identifying the risk assessment process implemented by the auditee to identify, analyze, and manage relevant risks.
- Information and communication – This includes the entity’s processes to identify, capture, and communicate to appropriate personnel the necessary information in a timely manner. The information may be manual or automated and may be from internal or external sources.
- Control activities – This includes policies and procedures that help ensure that management directives are carried out. Examples would be approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
- Monitoring – This includes the types of activities the entity uses to keep an eye on internal controls. These activities may be accomplished through ongoing processes and periodic reviews.

The evaluation of the internal control environment should provide reasonable, but not absolute, assurance that the fundamental elements of the processes are sufficient to accomplish their intended purpose. The evaluation should be adequately documented and properly supported by the results of tests, observations, and inquiries. The use of information systems that can affect the reliability, accuracy, or usefulness of financial or statistical data and reports should be included as part of the evaluation.

This evaluation may be done by using one or a combination of methods, such as interviews with unit personnel, completion of an internal control questionnaire, walk-through or re-performance of transactions, or creation of flowcharts. A conclusion on the overall internal control environment of the unit being audited and the results of testing must be included in the working papers.

Entrance Conference

Before any work formally commences on an audit, the UW System internal auditor will notify the auditee, which is normally defined as the most senior manager directly responsible or accountable for the function, program, activity, department, or unit being audited. In some cases, there may be a shared accountability or an intersection of line and functional authority. In these cases, more than one auditee will be identified and informed of the audit.

The notification may be made verbally or in writing, and specifies information known at the outset of the audit, such as the initial objectives, scope, and any specific

considerations or concerns. The internal auditor or the auditee may also request the scheduling of an entrance conference, which is an opportunity to establish the proper atmosphere and to begin building good working relationships.

The purpose of an entrance conference is to discuss the plans for the overall conduct of the audit. During the entrance conference, the internal auditor will:

- explain the type of audit being undertaken, the scope of the planned audit, the audit objectives, the period to be audited, and the general approach to the audit;
- verify that the auditee understands the role of the internal auditor(s) and the commitment needed from the auditee to support the audit and respond to audit requests;
- ask the appropriate members of management if they have any particular areas of risk or concern which they would like reviewed;
- request management plans, objectives, or other documents that may have a material impact on the audit outcome;
- confirm the location of documents and records needed during the audit;
- review audit findings from previous internal or external audits, if applicable, and the current status of corrective actions;
- develop a list of key personnel in the auditee department to be contacted for meetings or information;
- discuss the procedure for preparing and reviewing the formal audit report;
- inquire about current developments relating to the function, program, activity, department, or unit under audit;
- explain the preliminary audit program in general terms and establish priorities for the audit; and
- discuss any other applicable topics.

UW System internal auditors may choose to provide no advance notification of the audit or review and not schedule an entrance conference for some audits, such as cash counts and when fraud, abuse, or financial irregularities are suspected.

CHAPTER IV

Audit Evidence

Evidential matter obtained during the course of an audit provides the documented basis for the internal auditor's opinions, findings, and recommendations as expressed in the audit report. As a result, UW System internal auditors are obligated to act objectively and collect sufficient, competent, relevant, and useful information during all audits.

Standards of Evidence

Audit procedures should be planned and performed to obtain sufficient and appropriate evidence so that audit risk will be limited to a level that is appropriate, in the auditor's professional opinion, for the audit in question. Sufficiency is the presence of enough factual and convincing evidence to support the auditor's findings, conclusions, and recommendations. It refers to both quality and quantity of evidence. Appropriateness means that the audit evidence is relevant and reliable. Some sources of evidence are more reliable than others. For example:

- Evidence obtained from an independent source (outside the auditee) is generally more reliable than that secured from the auditee.
- Evidence developed under effective internal controls is more reliable than that obtained where controls are weak or nonexistent.
- Evidence obtained through the internal auditor's direct personal knowledge, such as through observation, computation, or inspection, is more reliable than evidence obtained indirectly, such as through verbal or written representation.
- Original documents are more reliable than copies.

The concept of sufficiency and reasonableness recognizes that internal auditors can never reduce audit risk to zero. The accumulation of evidence must be persuasive. The internal auditor should decide what evidence is available within the limits of time and cost to support their opinion and conclusions.

The internal auditor should be able to prove by documented evidence that an opinion is based on a pattern of activity or inactivity, or on existing circumstances that caused or failed to prevent an isolated problem from occurring. Depending on the circumstances, working papers that contain copies of several examples of deficiencies may be sufficient to establish a pattern, rather than copying every instance of the problem. A reference must be made as to the location and identification of documents not copied so they can be examined at a later date, should that be necessary.

Types of Evidence

Internal auditors generally gather evidence from internal staff, information systems, and documents, which may require verification from external sources. In addition to staff, some internal sources of audit evidence include books of account, ledgers and records,

memoranda, minutes of meetings, system-generated reports, and documents that support transactions. Information gathered from these sources may be verified from external sources that include confirmations of bank balances, accounts receivable, and assets held by third parties.

All of the information gathered to support the internal audit effort, and the conclusions drawn therefrom, should be considered audit evidence which may be categorized as:

- Documentary evidence - “created” information, such as letters, contracts, accounting records, screen prints, system-generated reports, and invoices.
- Physical evidence - obtained by direct inspection or observation of activities, property, or events.
- Testimonial evidence - obtained from others through statements received in response to inquiries or through interviews. The statements critical to the audit should be corroborated through independent verification when feasible.
- Analytical Evidence - compiled by the auditor from other types of evidence and includes computations and comparisons.

Types of Audit Procedures

All audits involve some type of testing. The audit objectives and the internal auditors’ understanding of internal controls and risks should be used in determining the nature, timing, and extent of control, substantive, and/or compliance tests. Common types of evidence collection procedures include, but are not limited to:

- Confirmation – obtaining primarily written, and sometimes oral, responses from third parties regarding particular items, such as bank balances.
- Physical examination – inspecting/counting tangible asset or reviewing documents and records.
- Vouching/Tracing – following source documents to the accounting, IT, or other records or vice versa.
- Recalculation – verifying mathematical accuracy of computations.
- Re-performance – performing transactions or tasks using the same methods as individuals who normally perform the transaction or task.
- Inquiry – obtaining information by asking questions through interviews or surveys.
- Observation – viewing tasks performed by the auditee to understand who performs them, how they are performed, and when.
- Reconciliation – matching two independent sources of information.
- Analytical procedures – using comparisons and relationships to determine whether balances or amounts appear reasonable.

The list of evidence collection procedures provided above is not intended to be all inclusive. Depending on the circumstances, UW System internal auditors may choose to use procedures not included in the list.

Sampling

In today's auditing environment, internal auditors seldom perform audit tests on all items in an account balance or class of transactions for the purpose of evaluating some characteristic of the population. Instead, audit sampling is employed. Audit sampling is performing an audit test on less than 100% of a population to determine parameters and characteristics of the whole population, with the auditor accepting the risk that some or all errors will not be found and the conclusions drawn (e.g., all transactions were proper and accurate) may be incorrect.

Determining whether or not to use audit sampling depends on the objective(s) to be achieved by the procedure. When audit sampling is desired, the internal auditor must choose between statistical and non-statistical sampling. Non-statistical sampling, which can be random or judgmental, is sampling without particular regard to the parameters of a statistical sample. A procedure calling for an audit sample with the objective of drawing conclusions regarding the whole population would require a statistical sample. Another factor to consider would be the cost effectiveness of using statistical sampling. For example, statistical sampling would not be feasible when sampling a relatively small population. Ultimately, the internal auditor should rely on sound audit judgment in determining which method to use.

Non-statistical sampling methods may be used when any of the following criteria apply:

- They are designed to be equally or more effective and efficient as statistical sampling, while being less costly.
- An internal auditor encounters a well-designed, well-controlled system, good management, well-trained employees and a feedback mechanism that highlights errors. In this case, the time and effort needed for a statistical sample may be excessive.
- An internal auditor encounters a system that is so weak (e.g. inadequate controls and/or procedures, insufficiently trained personnel) that no reliance can be placed on the system of internal controls. In this case, the time and effort needed for a statistical sample may be excessive.
- The audit objectives are fully met by a non-statistical sample.
- It is known that the population has no variability.
- Examples of deficiencies are needed to support the auditor's contention that the system is weak.
- Clues are needed as to whether to proceed with a statistical sample.

Statistical sampling methods, though used less frequently, may be used when any of the following criteria apply:

- Cost-benefit analyses support the additional costs and time required.
- The sample errors or exceptions must be extrapolated to the population, or a defensible expression of the test results is required.

- The objective of the audit is to state an opinion on the reliability of the balances reported.
- With the availability of computer software for sampling, they would be simpler to apply.
- The risk of a sampling error must be quantified.

There are several methods that can be used to select a sample including haphazard selection, judgmental sampling, random number sampling, and systematic/interval sampling. The haphazard selection method is similar to selecting items from a hat. Items are selected without bias of color, size, location, etc. This may be difficult as people generally are unconsciously aware of these factors. With judgmental sampling, the auditor chooses a sample based on risk factors, such as dollar amount or category. Random number sampling tools, such as Excel random function, may be used to assist in the identification of the random sample. The most common form of systematic sampling is when every n^{th} item is selected for review. Systematic sampling can only be applied if the given population is homogeneous.

Finally, as previously noted in this manual, the extent and scope of sampling should be clearly stated at every phase of the audit to which it is applied; accordingly, the working papers will disclose the character and extent of all sampling methods utilized.

CHAPTER V

Concluding the Audit

In the final stages of an audit, the UW System internal auditor should review all evidence obtained to ensure it is sufficient to support conclusions and recommendations. In doing this, internal auditors should evaluate identified findings, assess procedures performed during the audit to address risks, and consider whether any additional work is needed. At this point, the internal auditor also begins the reporting phase, which includes summarizing the findings for the auditee, drafting the report, issuing initial and subsequent drafts, reviewing management action plans, and preparing and distributing the final audit report.

Evaluating Audit Issues and Tracking Findings

Potential audit issues are evaluated as part of the end-of-audit and reporting processes. The issues may relate to control deficiencies; known and likely misstatements; instances of noncompliance with laws, regulations, contracts, or grant agreements; and fraud or abuse. As potential audit issues are identified and as the audit nears conclusion, the internal auditor should consider what steps need to be taken for each issue.

Audit issues for which a recommendation is made (verbally or written) are commonly referred to as audit findings. Well-developed audit findings, regardless of the subject matter, have certain common attributes: criteria, condition, cause, effect, and recommendation. These attributes, which should be documented in audit working papers, help evaluate the exception's significance, identify related exceptions, and provide an easy transition from working papers to the report. If one or more of these attributes are missing, questions regarding the soundness of the audit finding may be raised.

It is important for the internal auditor to track audit findings identified during the audit. The aggregation of findings helps the auditor when assessing the pervasiveness and significance of the issues identified, which is useful in classifying deficiencies identified. Tracking audit findings also helps ensure all audit issues are properly reported to management and identifies issues requiring follow-up during subsequent audits.

It is often helpful to track audit findings in a separate summary working paper, which:

- indicates the nature of the finding;
- references the working paper where the exception was noted; and
- indicates whether the exception was reported in the audit report or discussed at the exit conference.

Deficiencies identified during the audit should be discussed with the auditee to verify the facts before any audit reports are drafted. If these discussions confirm that a deficiency exists, the internal auditor will draft a preliminary report. All findings will be considered preliminary unless (and until) they are included in the final audit report.

Exit Conference

The purpose of an exit conference with the auditee is to develop a mutual understanding of the content of the audit report. This should avoid any misunderstandings or misinterpretations of fact by providing the opportunity for the auditee to clarify specific items and to express views on the corrective action and other information presented in the draft report.

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

The discussion topics at each exit conference will vary depending on several factors, including audit concerns noted and the exit conference attendees. At a minimum, the internal auditor should be prepared to discuss the audit objectives, scope, and procedures; the perceived audit risks; the audit conclusions reached; the corrective actions being recommended, if any; and any other concerns identified during the audit.

During the exit conference, the auditee may present additional information or request wording changes to the draft audit report. If significant changes are needed, a revised report draft should be provided to the auditee.

Communicating Audit Findings

Internal audit is intended to provide added assurance on risk management, control and governance processes. In order to accomplish this objective, audit conclusions and recommendations must be effectively communicated to the auditee. The timing and type of communication may vary depending on the type of audit, the intended audience, the needs of the auditee, and the significance of the issues identified.

All written audit communication must be clear and precise to ensure that the reader will understand what the report is trying to achieve. Reports should be fair, balanced, and presented in an unbiased tone, noting where management has taken actions to correct deficiencies and pointing out exemplary performance. Reports are normally more effective when related observations can be aggregated and addressed with higher-level recommendations, e.g. to improve controls.


Only matters of significance should be included in the report – thus not all observations and recommendations recorded during the audit will be brought forward to the report. The UW System internal auditor should finalize a log of all misstatements or findings noted during the audit. If an audit issue will not be formally communicated to the institutional administration, an explanation for this decision should be documented.

Written communication may occur during the course of the audit. Prior to issuing the final report, the internal auditor may utilize interim reports to communicate information that requires immediate attention, communicate a change in audit scope for the activity under review, or to keep management informed of audit progress when audits extend over a long period.

At the completion of each audit, the internal auditor should issue a written report, addressed to appropriate institutional management, to communicate the audit's results. Every attempt should be made to make the report accurate, objective, clear, concise, constructive, timely, and complete. The report should include the audit objectives and scope, as well as applicable conclusions, recommendations, and responses and corrective action plans.

The interim audit memos, final audit report or management letter, and other supplemental communications with institutional management should be indexed and cross-referenced to supporting working papers. Copies of the issued memos, management letter, and/or audit report should be maintained for future reference. The UW System internal auditors should discard any hard-copy and/or electronic copy of unnecessary documents and discard temporary working copies which have been finalized in the permanent working paper files.

Audit communication should note that the report is intended solely for the information and use of management of the UW institution and is not intended to be used by others. However, internal audit reports are considered public records. Therefore, the distribution and use of the results cannot be restricted. If open records requests are received, they should be forwarded to the institutional public records custodian to determine how the request will be fulfilled.



CHAPTER VIII

Investigative Audits

Investigative audits focus on alleged civil or criminal violations of state or federal laws and violations of University policies and procedures that may result in prosecution or disciplinary action. Allegations of theft, misuse of University assets, and conflicts of interest are examples of reasons for investigative audits. To avoid damaging the reputation of innocent persons suspected of wrongful conduct and to protect the UW System from potential civil liability, it is crucial that confidentiality be maintained during these audits.

Investigative audits may be initiated as a result of routine audit procedures, a staff complaint – possibly anonymous, or a request from University management or campus police. During each audit, UW System internal auditors should continually be alert to the possibility of fraudulent activities. This requires that internal auditors be trained to recognize conditions and activities that promote the occurrence of fraudulent activities. This recognition can be sharpened by a thorough understanding of the area being audited; knowledge of any laws, rules, regulations, policies or procedures that may govern the operation; and awareness of the internal controls that one would expect to effectively administer the operation. Indicators of fraudulent activity may include weak controls; noncompliance with laws, rules and regulations, and policies and procedures; and inadequate or unusual financial records or documents.

Objectives

The objectives of investigative audits are to determine whether the fiscal or compliance breach occurred, determine and document the magnitude of the breach, identify the responsible individual(s), and provide recommendations for corrective actions to improve prevention and detection procedures including, when necessary, recommendations that call for immediate action to prevent further losses (e.g., reassignment of duties, suspension, or discharge, depending on the circumstances).

Procedures

UW System Financial Policy F16, *Breach of Fiscal Integrity*, delineates the procedures to follow when there is any indication of actual or suspected theft, embezzlement, falsification of documents, or conflicts of interest (see <http://www.uwsa.edu/fadmin/fppp/fppp16.htm>). According to F16:

1. The discovering party should immediately notify the unit business officer of the situation, who should immediately notify the respective chancellor and UW System Vice President for Finance.
2. The UW System Office of Operations Review and Audit, in cooperation with appropriate institutional officials, will investigate the matter and determine if audit assistance is necessary. Institutional officials may include, but are not limited to, the chief business officer, internal auditor, campus police, and legal counsel.

3. Following a full investigation, determination will be made by the UW System Administration's Office of General Counsel, Office of Operations Review and Audit, and institutional offices as to whether the Department of Justice should be notified. In some cases, it may be appropriate to notify the District Attorney's Office in the county where the campus is located (instead of or in addition to the Department of Justice).
4. The Department of Justice or District Attorney will advise as to what, if any, criminal laws have been violated and what additional investigation may be necessary.
5. If federal funds are involved, appropriate federal authorities will be notified.

Some UW institutions have their own policies and/or procedures regarding breaches of fiscal integrity and the resulting investigative audits. In addition to F16, institutional internal auditors should consult these policies and procedures as well, to help ensure institutional processes are followed and appropriate staff are notified.

Specific audit procedures will be dictated by the circumstances and may not be shared with the auditee. However, the information that is reviewed and analyzed during an investigative audit may be presented in a court of law. As a result, the following guidelines should be followed:

- Strict confidentiality is required during all investigative audits. Information regarding the purpose of the audit and any tentative conclusions should be restricted to members of the investigation team.
- The allegation should be thoroughly understood so that records and other information required for the audit and necessary analyses may be identified.
- The records to be reviewed should be stored in a secured location to reduce the possibility of tampering prior to review. Access to this storage location should be restricted to internal audit and other appropriate staff.
- Assistance should be sought from other investigative team members in order to obtain or clarify information. For example, campus or local law enforcement may be able to obtain subpoenas and motor vehicle information.
- Working papers documenting our work should be prepared in accordance with standards identified in Chapter II of this manual. The preparation of concise, accurate, and unbiased working papers is crucial. The purpose, source, and conclusion must be clearly stated in each working paper.
- Records should be reviewed closely to verify their authenticity. The types of records or the information presented on these records may provide facts to support the veracity of the allegation. Examples of this may include the use of photocopies rather than original documents; information on documents that does not agree with the explanation of the transaction, such as date, time, or location variations; and vendor invoices that could have been prepared on any computer.
- Consideration should be given to recording certain interviews, with appropriate notice and consent of the parties involved.
- Where possible, information should be verified with other University departments or outside organizations, such as vendors.

- Original documentation must be maintained for transactions that have been identified as questionable. Photocopies of these original documents should be given to the office from where the document is taken. If necessary, these photocopies can be used by that department to continue its normal work. The original document should be dated and initialed by the auditor. A record showing the source of the document should be maintained.

UW System and Higher Education Key Terms, Acronyms, and Definitions

A133	OMB Circular A-133 – the federal regulations issued by OMB that set forth standards for the audit of States, local governments, and non-profit organizations expending federal awards
A21	OMB Circular A-21 – the federal regulations issued by OMB that establish principles for determining costs applicable to grants, contracts, and other agreements with educational institutions
ACUA	Association of College and University Auditors – an international professional organization serving institutions of higher education
ASSA	Academic Support Service Agreement – a procurement methodology that may be employed when the service is a unique, noncompetitive activity supporting instruction/research/public service
BOR	Board of Regents – governing body of the UW System; comprised of 18 members
CAFR	Comprehensive Annual Financial Report – the state government’s financial statements, which includes the UW System as an enterprise fund
CAU	Capital Accounting Unit in DOA – advises the State of Wisconsin Building Commission and the Governor on the issuance of state debt and administers finances for the clean water revolving loan fund program
CBO	Chief Business Officer – each campus has such a position, which generally oversees the controller and other business operations.
CSAO	Chief Student Affairs Officer – often an assistant vice chancellor position that is responsible for promoting student learning and development by providing services/programs that enhance student educational experiences
CSRG	Common Systems Review Group – a system-wide group established to oversee the implementation, maintenance, and cost of information technology systems used by all or the majority of institutions, such as SFS
DOA	Department of Administration – a State of Wisconsin cabinet agency that supports other state agencies and programs with services like centralized purchasing and financial management and assists the Governor in developing and implementing the state budget
DoIT	Division of Information Technology – a unit within UW-Madison that provides computer technology services to its campus and the UW System; responsible for the platforms on which SFS runs
DSF	Division of State Facilities – a unit within DOA that controls many of the capital programs operating state-wide
ECSI	Education Computer Systems, Inc. – an external UW service organization that manages several campuses’ loan programs
ERM	Enterprise Risk Management – a process used to identify, evaluate, prioritize, and manage risks inherent in UW operations
FAP	Financial and Administrative Policy – policies issued by UW System (see website)

FERPA	Federal Educational Rights and Privacy Act – a federal law that applies to all schools that receive funds under an applicable program of the U.S. Department of Education; provides that educational institutions must provide students with access to their education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records; with several exceptions, schools must have a student's consent prior to the disclosure of education records.
FFEL	Federal Family Education Loan Program – a type of student loan available through the federal government
FISAP	Fiscal Operations Report and Application to Participate – a report that summarizes a campus' financial aid program activities for federal compliance
FPP	Financial Policies and Procedures – former UW System policies which are now referred to as FAP
FTE	Full time equivalent/enrollment – full time equivalent converts employee head counts since some may be less than 100%, which is a concept encountered in all state agencies; full time enrollment performs the same conversion for student head counts
FTO	Furlough Time Off – the payroll code used to track furlough time taken by an employee
GAPP	General Administration Policies and Procedures – former UW System policies which are now referred to as FAP
GPO	General Program Operations – involves the UW System's primary GPR and PR appropriations; the concept is to spend all available GPR dollars from this pool first, then shift remaining expenditures to PR appropriations
GPR	General Purpose Revenue – consists of general taxes, miscellaneous receipts and revenues collected by state agencies which are paid into a specific fund, lose their identity, and are then available for appropriation by the Legislature
HEAB	Wisconsin's Higher Education Aids Board – the state agency responsible for the oversight of the State's financial aid system for Wisconsin residents; administers tuition reciprocity agreements, tuition capitation contracts, and various grant, scholarship, and loan programs
HRS	Human Resources System – the Oracle/PeopleSoft software that will be used for human resource, benefit, and payroll business processes; initial implementation is anticipated in spring 2011
IAA	Identification, Authentication and Authorization – provides identity management and authentication services supporting the secure deployment of applications at UW-System institutions
IAM	Identify and Access Management –provides authentication and provisioning (authorization) services to applications
IIA	Institute of Internal Auditors – a professional organization for internal auditors; provides professional development opportunities, certification, research, and technical guidance
IPEDS	Integrated Postsecondary Education Data System -- a system of interrelated surveys conducted annually by the National Center for Education Statistics

(NCES) to gather data (enrollments, program completions, graduation rates, faculty and staff, finances, institutional prices, and student financial aid) from every higher education institution that participates in the federal student financial aid programs; the data is available to researchers and others through the [IPEDS Data Center](#).

ISIS	Integrated Student Information System – a PeopleSoft student system used by UW-Madison and other institutions to record tuition and fee balances and other academic tracking information; some institutions refer to this PeopleSoft module as Campus Solutions
ITMC	Information Technology Management Council – a system-wide group established to consider information technology matters of common interest among University of Wisconsin institutions
JAC	Joint Audit Committee – a legislative committee that may direct LAB to conduct audits/evaluations, receive and review reports issued by LAB, conduct hearings on LAB reports, and introduce legislation pertaining to LAB recommendations
JCOER	Joint Committee on Employment Relations – a legislative committee that oversees and approves state and UW employee wages, benefits, travel reimbursement rates, and personnel management regulations, including those established through negotiations with labor organizations
JFC	Joint Finance Committee – a legislative committee that is charged with the review of all state appropriations and revenues
LAB	Legislative Audit Bureau – a nonpartisan service agency that conducts audits/evaluations of state agency operations to ensure financial transactions are legal and proper and to determine whether programs are administered effectively, efficiently, and in accordance with the policies of the Legislature and the Governor
LFB	Legislative Fiscal Bureau – a nonpartisan service agency that provides fiscal and program information/analyses to the Wisconsin Legislature, its committees, and individual legislators and serves as staff to JAC; the primary focus of the Bureau is the State’s biennial budget
LTE	Limited term employee – a group of employees who are appointed to fill civil service positions that are temporary or temporarily vacant; LTEs are paid on an hourly basis and may not work more than 1,043 hours per year in each LTE position
NACUBO	National Association of College and University Business Officers – a professional organization for business officers within higher education
OPAR	Office of Policy Analysis and Research – a unit within UWSA that supports system-wide planning, policy development, and evaluation through the collection and analysis of data and that disseminates statistical reports for internal and external use
OMB	Office of Management and Budget – a federal agency whose predominant mission is to oversee the preparation of the federal budget and to supervise its administration in Executive Branch agencies

OSLP	Office of Safety and Loss Prevention – a unit within UWSA that provides guidance to UW institutions for maintaining a safe, healthy environment for faculty, staff, students and others using UW programs and facilities
P-card	Purchasing Card – a charge card issued to an authorized UW employee (permanent, project, or LTE), by the campus, through the Master Agreement between the State of Wisconsin and US Bank.
PIR	Payment to Individual Report – the required mechanism for making payment to a non-employee or individual that is "a person who is not a company, partnership, corporation, association, organization, trust or estate, and for whom an employer-employee relationship does not exist."
PR	Program Revenue – consists of revenues that credited to an appropriation to finance a specified program or state agency.
RFB	Request for Bid – a competitive procurement process where there are well established specifications and an award is made to the low bidder that meets the specifications
RFP	Request for Proposal – a competitive procurement process involving the solicitation of proposals when an award cannot be made strictly on specifications or price and several firms are qualified to furnish the product or service; this process typically involves an evaluation team that scores the proposals
RPD	Regent Policy Document – policies adopted pursuant to the policy-making authority vested in the Board of Regents by Chapter 36 of the Wisconsin Statutes
RSP	Research & Sponsored Programs –a division of UW-Madison, organized within the Graduate School, which tracks compliance with gifts, grants, and contracts from local, state, federal, and private sources.
SBC	State Building Commission – approves funding and capital plans for advancement to the biennial budget process
SCO	State Controller’s Office – a unit within DOA that establishes accounting policies and procedures, maintains the state's central payroll and accounting systems, monitors agency internal control procedures, and produces the state's annual fiscal and financial reports
SEG	Segregated Revenue – consists of revenues which, by law, are deposited into funds other than the general fund and are available for the purposes for which such funds are created
SFS	Shared Financial System – the official accounting system of the UW System
T-card	Travel card – a credit card that provides an alternate method of payment for official, state business travel expenses
TER	Travel Expense Report – a form used to request and approve reimbursement of travel costs
UAS	University Accounting Services – an external UW service organization that manages several campuses’ loan programs.
UBIT	Unrelated Business Income Tax – a tax required from typically tax-exempt organizations if the revenue-generating activity is not substantially related to the UW institution’s mission

UDDS	Unit-division-department-sub department – this was an old department identifier that pre-dates SFS. For SFS purposes, the unit is the campus, and the DDS portion is the department id (DeptID).
UPG	Unclassified Personnel Guidelines – provides a systemwide framework for title usage, describes UWSA and UW institution authority for assignment of unclassified titles, offers general descriptions of unclassified titles, and furnishes each institution with the official list of title codes for budget and payroll purposes; the BOR is charged by statute with administering unclassified employment and the UPGs are meant to provide guidance to do so
UWSA	UW System Administration – UW entity that helps to develop, and then implements, monitors, and evaluates policies enacted by the Board of Regents, aligning university programs with the current and future needs of the state and the nation
WARF	Wisconsin Alumni Research Foundation – this is an affiliated organization of UW-Madison. This may also be used in reference to campuses which previously used information systems that have since been phased out (e.g. “WARF campuses”)
WiSDM	Wisconsin Data Mart – a web-based financial data access tool; WISDM is updated nightly with PeopleSoft Financial data
WiSMART	Wisconsin State Management Reporting & Accounting Tool – the official accounting system for the State of Wisconsin; information from the UW System’s SFS is uploaded to WiSMART
WiSys	Wisconsin System Technology Foundation – a non-profit, non-stock corporation designated by UW System to promote research and development at non-Madison campuses by moving university discoveries to industry through intellectual property protection and marketing
ZBA	Zero Balance Account – a checking account for a business unit’s check-writing operation; in order to maintain a zero balance, balances are swept in and out of the business unit account on a daily basis to the ‘parent’ account, which holds the cash