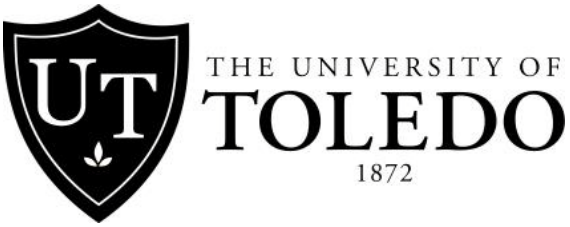

INTERNAL AUDIT DEPARTMENT

POLICY MANUAL

As of May 11, 2010

Issued: December, 2009
Revised:

Table of Contents

Internal Audit Charter (Purpose, Authority, and Responsibility)

The purpose, authority, and responsibility of The University of Toledo Internal Audit activity is formally defined in the Internal Audit Charter, consistent with the definition of internal auditing, The University of Toledo and Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*. The Director of Internal Audit periodically reviews the Internal Audit Charter and presents it to senior management and the Audit Committee of the Board of Trustees for approval.

The Internal Audit Charter is a formal document that defines the Internal Audit Department's purpose, authority, and responsibility. The Internal Audit Charter establishes the Internal Audit Department's position within the University; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. Final approval of the Internal Audit Charter resides with the Audit Committee.

The formal, written Internal Audit Charter is critical in managing the Internal Audit Department. The Internal Audit Charter provides a recognized statement for review and acceptance by management and for approval, as documented in the minutes, by the Audit Committee. It also facilitates a periodic assessment of the adequacy of the Internal Audit Department's purpose, authority, and responsibility, which establishes the role of the Internal Audit Department. If a question should arise, the Internal Audit Charter provides a formal, written agreement with management and the Audit Committee about The University's Internal Audit Department.

The Director of Internal Audit is responsible for periodically assessing whether the Internal Audit Department's purpose, authority, and responsibility, as defined in the Internal Audit Charter, continue to be adequate to enable the Department to accomplish its objectives. The Director of Internal Audit is also responsible for communicating the result of this assessment to senior management and the Audit Committee.

University Independence

The Director of Internal Audit reports to a level within the University that allows the Internal Audit Department to fulfill its responsibilities. The Director of Internal Audit must confirm to the Audit Committee, at least annually, the organizational independence of the Internal Audit Department.

Support from senior management and the Audit Committee assists the Internal Audit Department in gaining the cooperation of engagement clients and performing their work free from interference.

The Director of Internal Audit, reporting functionally to the Audit Committee and administratively to The University's Chief Financial Officer (with unfettered access to The University's President), facilitates University independence. Thus, the Director of Internal Audit reports to an individual in the University with sufficient authority to promote independence and to ensure broad audit coverage, adequate consideration of engagement communications, and appropriate action on engagement recommendations.

Functional reporting to the Audit Committee typically involves the Audit Committee:

- Approving the Internal Audit Department's overall Charter.
- Approving the internal audit risk assessment and related audit plan.
- Receiving communications from the Director of Internal Audit on the results of the internal audit activities or other matters that the Director of Internal Audit determines are necessary, including private meetings with the Director of Internal Audit without management present, as well as annual confirmation of the Internal Audit Department's University independence.
- Approving all decisions regarding the performance evaluation, appointment, or removal of the Director of Internal Audit.
- Approving the annual compensation and salary adjustment of the Director of Internal Audit.
- Making appropriate inquiries of management and the Director of Internal Audit to determine whether there is audit scope or budgetary limitations that impede the ability of the Internal Audit Department to execute its responsibilities.

Administrative reporting is the reporting relationship within The University's management structure that facilitates the day-to-day operations of the Internal Audit Department. Administrative reporting typically includes:

- Budgeting and management accounting.
- Human resource administration, including personnel evaluations and compensation.
- Internal communications and information flows.
- Administration of the Internal Audit Department's policies and procedures.

Audit Committee Interaction

The Director of Internal Audit communicates and interacts directly with the Audit Committee.

Direct communication occurs when the Director of Internal Audit regularly attends and participates in Audit Committee meetings that relate to the Board of Trustees' oversight responsibilities for auditing, financial reporting, University governance, and control. The Director of Internal Audit's attendance and participation at these meetings provide an opportunity to be apprised of strategic business and operational developments, and to raise high-level risk, systems, procedures, or control issues at an early stage. Meeting attendance also provides an opportunity to exchange information concerning the Internal Audit Department's plans and activities and to keep each other informed on any other matters of mutual interest.

Such communication and interaction also occurs when the Director of Internal Audit meets privately with the Audit Committee, at least annually.

Individual Objectivity

The University of Toledo internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

Conflict of interest is a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfill his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the Internal Audit Department, and the profession. A conflict of interest could impair an individual's ability to perform his or her duties and responsibilities objectively.

Individual objectivity means the internal auditors perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Internal auditors are not to be placed in situations that could impair their ability to make objective professional judgments.

Individual objectivity involves the Director of Internal Audit organizing staff assignments that prevent potential and actual conflict of interest and bias, periodically obtaining information from the internal audit staff concerning potential conflict of interest and bias, and, when practicable, rotating internal audit staff assignments periodically.

The occasional performance of non-audit work by the internal auditor, with full disclosure in the reporting process, would not necessarily impair objectivity. However, it would require careful consideration by management and the Director of Internal Audit to avoid adversely affecting the internal auditor's objectivity.

Impairment to Independence or Objectivity

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

Impairment to University independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding**.**
The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations of the Internal Audit Department's, the Chief Financial Officer's, and the President's responsibilities to senior management and the Audit Committee as described in the Internal Audit Charter, as well as the nature of the impairment.

Internal auditors are to report to the Director of Internal Audit any situations in which an actual or potential impairment to independence or objectivity may reasonably be inferred, or if they have questions about whether a situation constitutes impairment to objectivity or independence. If the Director of Internal Audit determines that impairment exists or may be inferred, he or she will reassign the auditor(s).

A scope limitation is a restriction placed on the Internal Audit Department that precludes the Department from accomplishing its objectives and plans. Among other things, a scope limitation may restrict the:

- Scope defined in the Internal Audit Charter.
- Internal Audit Department's access to records, personnel, and physical properties relevant to the performance of engagements.
- Approved engagement work schedule.
- Performance of necessary engagement procedures.

- Approved staffing plan and financial budget.

A scope limitation, along with its potential effect, will be communicated, preferably in writing, to the Audit Committee. The Director of Internal Audit will consider whether it is appropriate to inform the Audit Committee regarding scope limitations that were previously communicated to and accepted by the Audit Committee. This may be necessary particularly when there have been organization, Board of Trustee, senior management, or other changes.

Internal auditors are not to accept fees, gifts, or entertainment from an employee, client, customer, supplier, or business associate that may create the appearance that the auditor's objectivity has been impaired. The appearance that objectivity has been impaired will apply to current and future engagements conducted by the auditor. The status of engagements is not to be considered as justification for receiving fees, gifts, or entertainment. The receipt of promotional items (such as pens, calendars, or samples) that are available to employees and the general public and have minimal value do not hinder internal auditors' professional judgments. Internal auditors are to report immediately the offer of all material fees or gifts to their supervisors.

Assessing Operations for Which Internal Auditors Were Previously Responsible

The internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an auditor provides assurance services for an activity for which the auditor had responsibility within the previous year.

Persons transferred to, or temporarily engaged by, the Internal Audit Department should not be assigned to audit those activities they previously performed or for which they had management responsibility until at least one year has elapsed. Such assignments are presumed to impair objectivity, and additional consideration should be exercised when supervising the engagement work and communicating engagement results.

Internal Audit's Responsibility for Other (Non-audit) Functions

Assurance engagements for functions over which the Director of Internal Audit has responsibility must be overseen by a party outside the Internal Audit Department.

Internal auditors are not to accept responsibility for non-audit functions or duties that are subject to periodic internal audit assessments. If they have this responsibility, then they are not functioning as internal auditors.

When the Internal Audit Department, Director of Internal Audit, or individual internal auditor is responsible for, or management is considering assigning, an operational responsibility that the Internal Audit Department might audit, the internal auditor's independence and objectivity may be impaired. At a minimum, the Director of Internal Audit will consider the following factors in assessing the impact on independence and objectivity:

- Requirements of the University of Institute of Internal Auditors Code of Ethics and the *Standards for the Professional Practice of Internal Auditing*.
- Expectations of stakeholders that will include the taxpayers, Board of Trustees, management, legislative bodies, public entities, regulatory bodies, and public interest groups.
- Allowances and/or restrictions contained in the Internal Audit Charter.
- Disclosures required by the *Standards for the Professional Practice of Internal Auditing*.
- Audit coverage of the activities or responsibilities undertaken by the internal auditor.
- Significance of the operational function to the University (in terms of revenue, expenses, reputation, and influence).
- Length or duration of the assignment and scope of responsibility.
- Adequacy of separation of duties.
- Whether there is any history or other evidence that the internal auditor's objectivity may be at risk.

Since the Internal Audit Charter contains specific restrictions/limiting language regarding the assignment of non-audit functions to the internal auditor, disclosure and discussion with management of such restrictions is necessary. If management insists on such an assignment, then disclosure and discussion of this matter with the Audit Committee is necessary.

Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

Proficiency and due professional care are the responsibility of the Director of Internal Audit and each internal auditor. As such, the Director of Internal Audit ensures that persons assigned to each engagement collectively possess the necessary knowledge, skills, and other competencies to conduct the engagement appropriately.

Due professional care includes conforming with the Institute of Internal Auditors Code of Ethics and, as appropriate, the University's Code of Conduct as well as the codes of conduct for other professional designations the internal auditors may hold. The Institute of Internal Auditors Code of Ethics extends beyond the definition of internal auditing to include two essential components:

- Principles that are relevant to the profession and practice of internal auditing: integrity, objectivity, confidentiality, and competency.
- Rules of conduct that describe behavioral norms expected of internal auditors. These rules are an aid to interpreting the principles into practical applications and are intended to guide the ethical conduct of internal auditors.

Proficiency

The internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The Internal Audit Department collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Knowledge, skills, and other competencies is a collective term that refers to the professional proficiency required of internal auditors to effectively carry out their professional responsibilities. The Internal Auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations.

The knowledge, skills, and other competencies referred to in the standard include:

- Proficiency in applying internal audit standards, procedures, and techniques in performing engagements. Proficiency means the ability to apply knowledge to situations likely to be encountered and to deal with them appropriately without extensive recourse to technical research and assistance.
- Proficiency in accounting principles and techniques if internal auditors work extensively with financial records and reports.
- Knowledge to identify the indicators of fraud.

- Knowledge of key information technology risks and controls and available technology-based audit techniques.
- An understanding of management principles to recognize and evaluate the materiality and significance of deviations from good business practices. An understanding means the ability to apply broad knowledge to situations likely to be encountered, to recognize significant deviations, and to be able to carry out the research necessary to arrive at reasonable solutions.
- An appreciation of the fundamentals of business subjects such as accounting, economics, commercial law, finance, quantitative methods, information technology, risk management, and fraud. An appreciation means the ability to recognize the existence of problems or potential problems and to identify the additional research to be undertaken or the assistance to be obtained.
- Skills in dealing with people, understanding human relations, and maintaining satisfactory relationships with engagement clients.
- Skills in oral and written communications to clearly and effectively convey such matters as engagement objectives, evaluations, conclusions, and recommendations.

Suitable criteria of education and experience for filling Internal Audit positions is established by the Director of Internal Audit who gives due consideration to the scope of work and level of responsibility and obtains reasonable assurance as to each prospective auditor's qualifications and proficiency.

The Internal Audit Department must collectively possess the knowledge, skills, and other competencies essential to the practice of the profession within the University. Performing an annual analysis of the Internal Audit Department's knowledge, skills, and other competencies helps identify areas of opportunity that can be addressed by continuing professional development, recruiting, or co-sourcing.

Continuing professional development is essential to help ensure Internal Audit staff remains proficient.

The Director of Internal Audit will obtain assistance from experts outside the Internal Audit Department to support or complement areas where the Internal Audit Department is not sufficiently proficient.

Obtaining External Service Providers to Support or Complement the Internal Audit Department

The Director of Internal Audit must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Each member of the Internal Audit Department need not be qualified in all disciplines. The Internal Audit Department may use external service providers or internal resources that are qualified in disciplines such as accounting, auditing, economics, finance, statistics, information technology, engineering, law, environmental affairs, and other areas as needed to meet the Internal Audit Department's responsibilities.

An external service provider is a person or firm, independent of the University, who has special knowledge, skill, and experience in a particular discipline. External service providers include actuaries, accountants, appraisers, environmental specialists, fraud investigators, lawyers, engineers, geologists, security specialists, statisticians, information technology specialists, the University's external auditors, and other audit organizations. An external service provider may be engaged by the Audit Committee, senior management, or the Director of Internal Audit.

External service providers may be used by the Internal Audit Department in connection with, among other things:

- Achievement of the objectives in the engagement work schedule.
- Audit activities where a specialized skill and knowledge are needed such as information technology, or statistics.
- Valuations of assets such as land and buildings, works of art, precious gems, investments, and complex financial instruments.
- Determination of quantities or physical condition of certain assets.
- Measuring the work completed and to be completed on contracts in progress.
- Fraud and security investigations.
- Determinations of amounts, by using specialized methods such as actuarial determinations of employee benefit obligations.
- Interpretation of legal, technical, and regulatory requirements.
- Evaluation of the Internal Audit Department's quality assurance and improvement program in conformance with The Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing*.
- Mergers and acquisitions.
- Consulting on risk management and other matters.

When the Director of Internal Audit intends to use and rely on the work of an external service provider, the Director of Internal Audit must consider the competence,

independence, and objectivity of the external service provider as it relates to the particular assignment to be performed. The assessment of competency, independence, and objectivity is also needed when the external service provider is selected by senior management or the Audit Committee, and the Director of Internal Audit intends to use and rely on the external service provider's work. When the selection is made by others and the Director of Internal Audit's assessment determines that he or she should not use and rely on the work of the external service provider, communication of such results is needed to senior management or the Audit Committee, as appropriate.

The Director of Internal Audit determines that the external service provider possesses the necessary knowledge, skills, and other competencies to perform the engagement by considering:

- Professional certification, license, or other recognition of the external service provider's competence in the relevant discipline.
- Membership of the external service provider in an appropriate professional organization and adherence to that organization's code of ethics.
- The reputation of the external service provider. This will include contacting others familiar with the external service provider's work.
- The external service provider's experience in the type of work being considered.
- The extent of education and training received by the external service provider in disciplines that pertain to the particular engagement.
- The external service provider's knowledge and experience in the industries in which the University operates.

The Director of Internal Audit must assess the relationship of the external service provider to the University and to the Internal Audit Department to ensure that independence and objectivity are maintained throughout the engagement. In performing the assessment, the Director of Internal Audit verifies that there are no financial, organizational, or personal relationships that will prevent the external service provider from rendering impartial and unbiased judgments and opinions when performing or reporting on the engagement.

The Director of Internal Audit assesses the independence and objectivity of the external service provider by considering:

- The financial interest the external service provider may have in the University.
- The personal or professional affiliation the external service provider may have to the Audit Committee, senior management, or others within the University.

- The relationship the external service provider may have had with the University or the activities being reviewed.
- The extent of other ongoing services the external service provider may be performing for the University.
- Compensation or other incentives that the external service provider may have.

If the external service provider is also the University's external auditor and the nature of the engagement is extended audit services, the Director of Internal Audit must ascertain that work performed does not impair the external auditor's independence. Extended audit services refer to those services beyond the requirements of audit standards generally accepted by external auditors. If the University's external auditors act or appear to act as members of senior management, management, or as employees of the University, then their independence is impaired. Additionally, external auditors may provide the University with other services such as consulting. Independence will be assessed in relation to the full range of services provided to the University.

To ascertain that the scope of work is adequate for the purposes of the Internal Audit Department, the Director of Internal Audit obtains sufficient information regarding the scope of the external service provider's work. These and other matters must be documented in an engagement letter or contract. To accomplish this, the Director of Internal Audit reviews the following with the external service provider:

- Objectives and scope of work including deliverables and time frames.
- Specific matters expected to be covered in the engagement communications.
- Access to relevant records, personnel, and physical properties.
- Information regarding assumptions and procedures to be employed.
- Ownership and custody of engagement working papers, if applicable.
- Confidentiality and restrictions on information obtained during the engagement.
- Where applicable, conformance with The Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* and the Internal Audit Department's standards for working practices.

In reviewing the work of an external service provider, the Director of Internal Audit evaluates the adequacy of work performed, which includes sufficiency of information obtained to afford a reasonable basis for the conclusions reached and the resolution of exceptions or other unusual matters.

When the Director of Internal Audit issues engagement communications, and an external service provider was used, the Director of Internal Audit will, as appropriate, refer to such services provided. The external service provider must be informed and, if

appropriate, concurrence should be obtained before making such reference in engagement communications.

Due Professional Care

University of Toledo internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

Due professional care calls for the application of the care and skill expected of a reasonably prudent and competent internal auditor in the same or similar circumstances. Due professional care is therefore appropriate to the complexities of the engagement being performed. Exercising due professional care involves internal auditors being alert to the possibility of fraud, intentional wrongdoing, errors and omissions, inefficiency, waste, ineffectiveness, and conflicts of interest, as well as being alert to those conditions and activities where irregularities are most likely to occur. This also involves internal auditors identifying inadequate controls and recommending improvements to promote conformance with acceptable procedures and practices.

Due professional care implies reasonable care and competence, not infallibility or extraordinary performance. As such, due professional care requires the internal auditor to conduct examinations and verifications to a reasonable extent. Accordingly, internal auditors cannot give absolute assurance that noncompliance or irregularities do not exist. Nevertheless, the possibility of material irregularities or noncompliance will be considered whenever an internal auditor undertakes an internal audit assignment.

Continuing Professional Development

The University of Toledo Internal Auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

The University of Toledo Internal Auditors are responsible for continuing their education to enhance and maintain their proficiency. Internal auditors need to stay informed about improvements and current developments in internal audit standards, procedures, and techniques, including The Institute of Internal Auditor's International Professional Practices Framework guidance. Continuing professional education (CPE) may be obtained through membership, participation, and volunteering in professional organizations such as The Institute of Internal Auditors, Information Systems Audit and Control Association, and Ohio Society of Certified Public Accountants; attendance at

conferences, seminars, and in-house training programs; completion of college and self-study courses; and involvement in research projects.

The internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certification, such as the Certified Internal Auditor designation (and other designations offered by The IIA) and additional designations related to internal auditing.

The internal auditors are encouraged to pursue CPE (related to the University's activities and industries) to maintain their proficiency with regard to the governance, risk, and control processes of the University.

Internal auditors who perform specialized audit and consulting work — such as information technology, actuarial, or systems design — may undertake specialized CPE to allow them to perform their internal audit work with proficiency.

Internal auditors with professional certifications are responsible for obtaining sufficient CPE to satisfy requirements related to the professional certification held.

Internal auditors not presently holding appropriate certifications are encouraged to pursue an educational program and/or individual study to obtain professional certification.

Quality Assurance and Improvement Program

The Director of Internal Audit will develop and maintain a quality assurance and improvement program that covers all aspects of the Internal Audit Department.

A quality assurance and improvement program is designed to enable an evaluation of the Internal Audit Department's conformance with the definition of internal auditing and The Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* and an evaluation of whether internal auditors apply the Institute of Internal Auditors Code of Ethics. The program also assesses the efficiency and effectiveness of the Internal Audit Department and identifies opportunities for improvement.

The Director of Internal Audit is responsible for establishing an Internal Audit Department whose scope of work includes the activities in The Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* and in the definition of internal auditing. To ensure that this occurs, the Director of Internal Audit has developed and maintained a quality assurance and improvement program (QAIP).

The Director of Internal Audit is accountable for implementing processes designed to provide reasonable assurance to the various stakeholders that the Internal Audit Department:

- Performs in accordance with the Internal Audit Charter, which is consistent with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*.
- Operates in an effective and efficient manner.
- Is perceived by those stakeholders as adding value and improving the University's operations.

These processes include appropriate supervision, periodic internal assessments and ongoing monitoring of quality assurance, and periodic external assessments.

The QAIP is sufficiently comprehensive to encompass all aspects of operation and management of the Internal Audit Department, as found in the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, the *Standards for the Professional Practice of Internal Auditing,* and best practices of the profession. The QAIP process is performed by or under direct supervision of the Director of Internal Audit. The Director of Internal Audit will usually delegate most QAIP responsibilities to subordinates.

Requirements of the Quality Assurance and Improvement Program

The quality assurance and improvement program must include both internal and external assessments.

A quality assurance and improvement program (QAIP) is an ongoing and periodic assessment of the entire spectrum of audit and consulting work performed by the Internal Audit Department. These ongoing and periodic assessments are composed of rigorous, comprehensive processes; continuous supervision and testing of internal audit and consulting work; and periodic validations of conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*. This also includes ongoing measurements and analyses of performance metrics (e.g., internal audit plan accomplishment, cycle time, recommendations accepted, and customer satisfaction). If the assessments' results indicate areas for improvement by the Internal Audit Department, the Director of Internal Audit will implement the improvements through the QAIP.

Assessments evaluate and conclude on the quality of the Internal Audit Department and lead to recommendations for appropriate improvements. QAIPs include an evaluation of:

- Conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*, including timely corrective actions to remedy any significant instances of nonconformance.
- Adequacy of the internal Audit Department's Charter, goals, objectives, policies, and procedures.
- Contribution to the University's governance, risk management, and control processes.
- Compliance with applicable laws, regulations, and government or industry standards.
- Effectiveness of continuous improvement activities and adoption of best practices.
- The extent to which the Internal Audit Department adds value and improves the University's operations.

The QAIP efforts also include follow-up on recommendations involving appropriate and timely modification of resources, technology, processes, and procedures.

To provide accountability and transparency, the Director of Internal Audit communicates the results of external and, as appropriate, internal quality program assessments to the various stakeholders of the Department (such as senior management, the Audit Committee, and external auditors). At least annually, the Director of Internal Audit reports to senior management and the Audit Committee on the quality program efforts and results.

Internal Assessments

Internal assessments will include:

- Ongoing monitoring of the performance of the Internal Audit Department; and
- Periodic reviews performed through self-assessment or by other persons within the University with sufficient knowledge of internal audit practices.

Ongoing monitoring is an integral part of the day-to-day supervision, review, and measurement of the Internal Audit Department. Ongoing monitoring is incorporated into the routine policies and practices used to manage the Internal Audit Department and

uses processes, tools, and information considered necessary to evaluate conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*.

Periodic reviews are assessments conducted to evaluate conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*.

Sufficient knowledge of internal audit practices requires at least an understanding of all elements of the Institute of Internal Auditors *International Professional Practices Framework*.

The processes and tools used in ongoing internal assessments include:

- Engagement supervision,
- Checklists and procedures (e.g., in an audit and procedures manual) are being followed,
- Feedback from audit customers and other stakeholders,
- Selective peer reviews of work papers by staff not involved in the respective audits,
- Project budgets, timekeeping systems, audit plan completion, and cost recoveries, and/or
- Analyses of other performance metrics (such as cycle time and recommendations accepted).

Conclusions are developed as to the quality of ongoing performance and follow-up action taken to ensure appropriate improvements are implemented.

The IIA's *Quality Assessment Manual*, or a comparable set of guidance and tools, will serve as the basis for periodic internal assessments.

Periodic internal assessments will:

- Include more in-depth interviews and surveys of stakeholder groups.
- Be performed by members of the Internal Audit Department (self-assessment).
- Be performed by Certified Internal Auditors (CIAs) or other competent audit professionals, currently assigned elsewhere in the University.
- Encompass a combination of self-assessment and preparation of materials subsequently reviewed by CIAs, or other competent audit professionals.

- Include benchmarking of the Internal Audit Department's practices and performance metrics against relevant best practices of the internal audit profession.

A periodic internal assessment performed within a short time before an external assessment can serve to facilitate and reduce the cost of the external assessment. If the periodic internal assessment is performed by a qualified, independent external reviewer or review team, the assessment results should not communicate any assurances on the outcome of the subsequent external quality assessment. The report may offer suggestions and recommendations to enhance the Internal Audit Department's practices. If the external assessment takes the form of a self-assessment with independent validation, the periodic internal assessment can serve as the self-assessment portion of this process.

Conclusions are developed as to quality of performance and appropriate action initiated to achieve improvements and conformity to the Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing,* as necessary.

The Director of Internal Audit will establish a structure for reporting results of internal assessments that maintains appropriate credibility and objectivity. Generally, those assigned responsibility for conducting ongoing and periodic reviews, report to the Director of Internal Audit while performing the reviews and communicate results directly to the Director of Internal Audit.

At least annually, the Director of Internal Audit reports the results of internal assessments, necessary action plans, and their successful implementation to senior management and the Audit Committee.

External Assessments

External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the University. The Director of Internal Audit must discuss with the Audit Committee:

- The need for more frequent external assessments.
- The qualifications and independence of the external reviewer or review team, including potential conflict of interest.

A qualified reviewer or review team consists of individuals who are competent in the professional practice of internal auditing and the external assessment process. The

evaluation of the competency of the reviewer and review team is a judgment that considers the professional internal audit experience and professional credentials of the individuals selected to perform the review. The evaluation of qualifications also considers the size and complexity of the organizations that the reviewers have been associated with in relation to the University's Internal Audit Department, as well as the need for particular sector, industry, or technical knowledge.

An independent reviewer or review team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the University.

External assessments cover the entire spectrum of audit and consulting work performed by the Internal Audit Department and should not be limited to assessing its quality assurance and improvement program. To achieve optimum benefits from an external assessment, the scope of work should include benchmarking, identification, and reporting of leading practices that could assist the Internal Audit Department in becoming more efficient and/or effective. This can be accomplished through either a full external assessment by a qualified, independent external reviewer or review team or a comprehensive internal self-assessment with independent validation by a qualified, independent external reviewer or review team
.
Nonetheless, the Director of Internal Audit will ensure the scope clearly states the expected deliverables of the external assessment in each case.

External assessments of the Internal Audit Department contain an expressed opinion as to the entire spectrum of assurance and consulting work performed (or that should have been performed based on the Internal Audit Charter) by the Internal Audit Department, including its conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing* and, as appropriate, includes recommendations for improvement. Apart from conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*, the scope of the assessment is adjusted at the discretion of the Director of Internal Audit, senior management, or the Audit Committee.

These assessments have considerable value to the Director of Internal Audit and other members of the Internal Audit Department, especially when benchmarking and best practices are shared.

On completion of the review, a formal communication is to be given to senior management and the Audit Committee.

There are two approaches to external assessments. The first approach is a full external assessment conducted by a qualified, independent external reviewer or review team. This approach involves an outside team of competent professionals under the leadership of an experienced and professional project manager. The second approach involves the use of a qualified, independent external reviewer or review team to conduct an independent validation of the internal self-assessment and a report completed by the Internal Audit Department**.** Independent external reviewers should be well versed in leading internal audit practices.

Individuals who perform the external assessment are free from any obligation to, or interest in, the University or the personnel of the University. Particular matters relating to independence, which will be considered by the Director of Internal Audit in consultation with the Audit Committee, in selecting a qualified, independent external reviewer or review team, include:

- Any real or apparent conflict of interest of firms that provide:
  - The external audit of financial statements.
  - Significant consulting services in the areas of governance, risk management, financial reporting, internal control, and other related areas.
  - Assistance to the Internal Audit Department. The significance and amount of work performed by the professional service provider is to be considered in the deliberation.
- Any real or apparent conflict of interest of former employees of the University who would perform the assessment. Consideration will be given to the length of time the individual has been independent of the University.
- Individuals who perform the assessment are independent of the University and do not have any real or apparent conflict of interest. “Independent of the organization” means not a part of, or under the control of, the University. In the selection of a qualified, independent external reviewer or review team, consideration will be given to any real or apparent conflict of interest the reviewer may have due to present or past relationships with the University or the Internal Audit Department, including the reviewer’s participation in internal quality assessments.
- Individuals in another department of the University or in a related university, although organizationally separate from the Internal Audit Department, are not considered independent for purposes of conducting an external assessment. A “related organization” may be an affiliate in the same group of entities.
- Real or apparent conflict involving peer review arrangements. Peer review arrangements between three or more universities (e.g., within a university or other affinity group, regional association, or other group of universities — except

as precluded by the "related organization" definition in the previous point) will be structured in a manner that alleviates independence concerns, but care is taken to ensure that the issue of independence does not arise. Peer reviews between two universities would not pass the independence test.

To overcome concerns of the appearance or reality of impairment of independence in instances such as those discussed in this section, one or more independent individuals could be part of the external assessment team to independently validate the work of that external assessment team.

Integrity requires reviewer(s) to be honest and candid within the constraints of confidentiality. Service and the public trust should not be subordinated to personal gain or advantage. Objectivity is a state of mind and a quality that lends value to a reviewer(s) services. The principle of objectivity imposes the obligation to be impartial, intellectually honest, and free of conflict of interest.

Performing and communicating the results of an external assessment require the exercise of professional judgment. Accordingly, an individual serving as an external reviewer should:

- Be a competent, certified internal audit professional that possesses current, in-depth knowledge of the Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing.*
- Be well versed in the best practices of the profession.
- Have at least three years of recent experience in the practice of internal auditing or related consulting at a management level.

Leaders of independent review teams and external reviewers who independently validate the results of the self-assessment should have an additional level of competence and experience gained from working previously as a team member on an external quality assessment, successful completion of The IIA's quality assessment training course or similar training, and director of internal audit or comparable senior internal audit management experience.

The reviewer(s) should possess relevant technical expertise and industry experience. Individuals with expertise in other specialized areas may assist the team. For example, specialists in enterprise risk management, IT auditing, statistical sampling, operations monitoring systems, or control self-assessment may participate in certain segments of the assessment.

The Director of Internal Audit involves senior management and the Audit Committee in determining the approach and selection of an external quality assessment provider.

The external assessment consists of a broad scope of coverage that includes the following elements of the Internal Audit Department:

- Conformance with the definition of internal auditing; the Institute of Internal Auditors Code of Ethics; and the *Standards for the Professional Practice of Internal Auditing*; and the Internal Audit Department's Charter, plans, policies, procedures, practices, and applicable legislative and regulatory requirements,
- Expectations of the Internal Audit Department expressed by the Audit Committee, senior management, and operational managers,
- Integration of the Internal Audit Department into the University's governance process, including the relationships between and among the key groups involved in the process,
- Tools and techniques employed by the Internal Audit Department,
- Mix of knowledge, experience, and disciplines within the staff, including staff focus on process improvement, and
- Determination as to whether or not the Internal Audit Department adds value and improves the University's operations.

The preliminary results of the review are discussed with the Director of Internal Audit during, and at the conclusion of, the assessment process. Final results are communicated to the Director of Internal Audit, or other official, who authorized the review for the University, preferably with copies sent directly to appropriate members of senior management and the Audit Committee.

The communication includes:

- An opinion on the Internal Audit Department's conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing* based on a structured rating process. The term "conformance" means the practices of the Internal Audit Department, taken as a whole, satisfy the requirements of the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*. Similarly, "nonconformance" means the impact and severity of the deficiencies in the practices of the Internal Audit Department are so significant they impair the Internal Audit Department's ability to discharge its responsibilities. The degree of "partial conformance" with the definition of internal auditing, the Institute of

Internal Auditors Code of Ethics, and/or individual standards, if relevant to the overall opinion, should also be expressed in the report on the independent assessment. The expression of an opinion on the results of the external assessment requires the application of sound business judgment, integrity, and due professional care.

- An assessment and evaluation of the use of best practices, both those observed during the assessment and others potentially applicable to the Department.
- Recommendations for improvement, where appropriate.
- Responses from the Director of Internal Audit that include an action plan and implementation dates.

To provide accountability and transparency, the Director of Internal Audit communicates the results of external quality assessments, including specifics of planned remedial actions for significant issues and subsequent information as to accomplishment of those planned actions, with the various stakeholders of the Department, such as senior management, the Audit Committee, and external auditors.

External Assessments: Self-assessment with Independent Validation

External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the University. The Director of Internal Audit must discuss with the Audit Committee:

- The need for more frequent external assessments.
- The qualifications and independence of the external reviewer or review team, including potential conflict of interest.

A qualified reviewer or review team consists of individuals who are competent in the professional practice of internal auditing and the external assessment process. The evaluation of the competency of the reviewer and review team is a judgment that considers the professional internal audit experience and professional credentials of the individuals selected to perform the review. The evaluation of qualifications also considers the size and complexity of the organizations that the reviewers have been associated with in relation to the University, as well as the need for particular sector, industry, or technical knowledge.

An independent reviewer or review team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the University.

A self-assessment with independent [external] validation includes:

- A comprehensive and fully documented self-assessment process, which emulates the external assessment process, at least with respect to evaluation of conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing.*
- An independent, on-site validation by a qualified, independent reviewer.
- Economical time and resource requirements — e.g., the primary focus would be on conformance with the Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing*.
- Limited attention to other areas — such as benchmarking, review and consultation as to employment of leading practices, and interviews with senior and operating management may be reduced. However, the information produced by these parts of the assessment is one of the benefits of an external assessment.

The same guidance and criteria would apply for a self-assessment with independent validation.

A team under the direction of the Director of Internal Audit performs and fully documents the self-assessment process. A draft report, similar to that for an external assessment, is prepared including the Director of Internal Audit's judgment on conformance with the Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing*.

A qualified, independent reviewer or review team performs sufficient tests of the self-assessment so as to validate the results and express the indicated level of the Department's conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*. The independent validation follows the process outlined in The IIA's *Quality Assessment Manual* or a similar comprehensive process.

As part of the independent validation, the independent external reviewer — upon completion of a rigorous review of the self-assessment team's evaluation of conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*:

- Reviews the draft report and attempts to reconcile unresolved issues (if any).
- If in agreement with the opinion of conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*, adds wording (as needed) to the

report, concurring with the self-assessment process and opinion and — to the extent deemed appropriate — in the report's findings, conclusions, and recommendations.
- If not in agreement with the evaluation, adds dissenting wording to the report, specifying the points of disagreement with it and — to the extent deemed appropriate — with the significant findings, conclusions, recommendations, and opinions in the report.
- Alternatively, may prepare a separate independent validation report — concurring or expressing disagreement as outlined above — to accompany the report of the self-assessment.

The final report(s) of the self-assessment with independent validation is signed by the self-assessment team and the qualified, independent external reviewer(s) and issued by the Director of Internal Audit to senior management and the Audit Committee.

To provide accountability and transparency, the Director of Internal Audit communicates the results of external quality assessments — including specifics of planned remedial actions for significant issues and subsequent information as to accomplishment of those planned actions — with the various stakeholders of the Department, such as senior management, the Audit Committee, and external auditors.

Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing"

The Director of Internal Audit may state that the internal Audit Department conforms with the Institute of Internal Auditors *International Standards for the Professional Practice of Internal Auditing* only if the results of the quality assurance and improvement program support this statement.

Ongoing monitoring and external and internal assessments of the Internal Audit Department are performed to evaluate and express an opinion as to the Internal Audit Department's conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing* and, as appropriate, should include recommendations for improvement.

The phrase to be used will be: "in conformance with the *Standards,*" or "in conformity to the *Standards*." To use one of these phrases, an external assessment is required at least once during each five-year period, along with ongoing monitoring and periodic internal assessments and these activities need to have concluded that the Internal Audit Department is in conformance with the definition of internal auditing, the Institute of

Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*.

Initial use of the conformance phrase is not appropriate until an external review has demonstrated that the Internal Audit Department is in conformance with the definition of internal auditing, the Institute of Internal Auditors Code of Ethics, and the *Standards for the Professional Practice of Internal Auditing*.

The Director of Internal Audit is responsible for disclosing instances of nonconformance that impact the overall scope or operation of the Internal Audit Department, including failure to obtain an external assessment within a five-year period, to senior management and the Audit Committee.

Before the Internal Audit Department's use of the conformance phrase, any instances of nonconformance that have been disclosed by a quality assessment (internal or external) which impair the Internal Audit Department's ability to discharge its responsibilities must be adequately remedied. In addition, the following are needed:

- Remedial actions need to be documented and reported to the relevant assessor(s) to obtain concurrence that the nonconformance has been adequately remedied, and
- Remedial actions and agreement of the relevant assessor(s) therewith need to be reported to senior management and the Audit Committee.

Linking the Audit Plan to Risk and Exposures

The Director of Internal Audit will establish risk-based plans to determine the priorities of the Internal Audit Department, consistent with the University's goals.

The Director of Internal Audit is responsible for developing a risk-based plan. The Director of Internal Audit takes into account the University's risk management framework, including using risk tolerance levels set by management for the different activities or parts of the University.

In developing the Internal Audit Department's audit plan, the Director of Internal Audit will first develop or update the audit universe. The audit universe is a list of all the possible audits that could be performed. The Director of Internal Audit will obtain input on the audit universe from senior management and the Audit Committee.

The audit universe can include components from the University's strategic plan. By incorporating components of the University's strategic plan, the audit universe will consider and reflect the overall business' objectives. Strategic plans also likely reflect the University's attitude toward risk and the degree of difficulty to achieving planned objectives. The audit universe will normally be influenced by the results of the risk management process. The University's strategic plan considers the environment in which the University operates. These same environmental factors would likely impact the audit universe and assessment of relative risk.

The Director of Internal Audit prepares the Internal Audit Department's audit plan based on the audit universe, input from senior management and the Audit Committee, and an assessment of risk and exposures affecting the University. Key audit objectives are usually to provide senior management and the Audit Committee with assurance and information to help them accomplish the University's objectives, including an assessment of the effectiveness of management's risk management activities.

The audit universe and related audit plan are updated to reflect changes in management direction, objectives, emphasis, and focus. It is advisable to assess the audit universe on at least an annual basis to reflect the most current strategies and direction of the University.

In some situations, audit plans may need to be updated more frequently (e.g., quarterly) in response to changes in the University's business, operations, programs, systems, and controls.

Audit work schedules are based on, among other factors, an assessment of risk and exposures. Prioritizing is needed to make decisions for applying resources. A variety of risk models exist to assist the Director of Internal Audit. Most risk models use risk factors such as impact, likelihood, materiality, asset liquidity, management competence, quality of and adherence to internal controls, degree of change or stability, timing and results of last audit engagement, complexity, and employee and government relations.

Using the Risk Management Process in Internal Audit Planning

The Director of Internal Audit will establish risk–based plans to determine the priorities of the Internal Audit Department, consistent with the University's goals.

Risk management is a critical part of providing sound governance that touches all the University's activities. Many universities are moving to adopt consistent and holistic risk management approaches that should, ideally, be fully integrated into the management

of the university. It applies at all levels — enterprise, function, and business unit — of the University. Management typically uses a risk management framework to conduct the assessment and document the assessment results.

An effective risk management process can assist in identifying key controls related to significant inherent risks. Enterprise risk management (ERM) is a term in common use.

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission defines ERM as "a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." Implementation of controls is one common method management can use to manage risk within its risk appetite. Internal auditors audit the key controls and provide assurance on the management of significant risks.

The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) defines control as "any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved."

Two fundamental risk concepts are inherent risk and residual risk (also known as current risk). Financial/external auditors have long had a concept of inherent risk that can be summarized as the susceptibility of information or data to a material misstatement, assuming that there are no related mitigating controls. The Institute of Internal Auditors *Standards for the Professional Practice of Internal Auditing* defines residual risk as "the risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk."

Current risk is often defined as the risk managed within existing controls or control systems.

Key controls can be defined as controls or groups of controls that help to reduce an otherwise unacceptable risk to a tolerable level. Controls can be most readily conceived as University processes that exist to address risks. In an effective risk management process (with adequate documentation), the key controls can be readily identified from the difference between inherent and residual risk across all affected systems that are relied upon to reduce the rating of significant risks. If a rating has not been given to inherent risk, the internal auditor estimates the inherent risk rating. When identifying key

controls (and assuming the internal auditor has concluded that the risk management process is mature and reliable), the internal auditor would look for:

- Individual risk factors where there is a significant reduction from inherent to residual risk (particularly if the inherent risk was very high). This highlights controls that are important to the University.
- Controls that serve to mitigate a large number of risks.

Internal audit planning will make use of the University risk management process, where one has been developed. In planning an engagement, the internal auditor considers the significant risks of the activity and the means by which management mitigates the risk to an acceptable level. The internal auditor uses risk assessment techniques in developing the Internal Audit Department's plan and in determining priorities for allocating Internal Audit resources. Risk assessment is used to examine auditable units and select areas for review to include in the Internal Audit Department's plan that have the greatest risk exposure.

Internal auditors may not be qualified to review every risk category and the ERM process in the University (e.g., internal audits of workplace health and safety, environmental auditing, or complex financial instruments). The Director of Internal Audit will ensure that internal auditors with specialized expertise or external service providers are used appropriately.

The maturity level of the University related to risk management varies among universities.

The role of this activity includes coordinating with management regarding its continuous review of the internal control structure and updating the structure according to evolving risk appetites. The internal auditors make an assessment of the University's risk management process and determine what parts can be used in developing the Internal Audit Department's plan and what parts can be used for planning individual internal audit assignments.

Factors the internal auditor considers when developing the internal audit plan include:

- Inherent risks — are they identified and assessed?
- Residual risks — are they identified and assessed?
- Mitigating controls, contingency plans, and monitoring activities — Are they linked to the individual events and/or risks?
- Risk registers — Are they systematic, completed, and accurate?

- Documentation — Are the risks and activities documented?

In addition, the internal auditor coordinates with other assurance providers and considers planned reliance on their work.

The Internal Audit Charter normally requires the Internal Audit Department to focus on areas of high risk, including both inherent and residual risk. The Internal Audit Department will identify areas of high inherent risks, high residual risks, and the key control systems upon which the University is most reliant. If the Internal Audit Department identifies areas of unacceptable residual risk, management will be notified so that the risk can be addressed. The internal auditor will, as a result of conducting a strategic audit planning process, be able to identify different kinds of activities to include in the Internal Audit Department's plan, including:

- Control reviews/assurance activities — where the internal auditor reviews the adequacy and efficiency of the control systems and provides assurance that the controls are working and the risks are effectively managed.
- Inquiry activities — where University management has an unacceptable level of uncertainty about the controls related to a business activity or identified risk area and the internal auditor performs procedures to gain a better understanding of the residual risk.
- Consulting activities — where the internal auditor advises University management in the development of the control systems to mitigate unacceptable current risks.

The internal auditors also try to identify unnecessary, redundant, excessive, or complex controls that inefficiently reduce risk. In these cases, the cost of the control may be greater than the benefit realized and therefore there is an opportunity for efficiency gains in the design of the control.

To ensure relevant risks are identified, the approach to risk identification is systematic and clearly documented. Documentation can range from the use of a spreadsheet to vendor supplied software. The crucial element is that the risk management framework is documented in its entirety.

The documentation of risk management in a university can be at various levels below the strategic level of the risk management process. The University has developed risk registers that document risks below the strategic level, providing documentation of significant risks in an area and related inherent and residual risk ratings, key controls, and mitigating factors. An alignment exercise can then be undertaken to identify more direct links between risk "categories" and "aspects" described in the risk registers and,

where applicable, the items already included in the audit universe documented by the Internal Audit Department.

The University has identified several high (or higher) inherent risk areas. While these risks may warrant the Internal Audit Department's attention, it is not always possible to review all of them. Where the risk register shows a high, or above, ranking for inherent risk in a particular area, and the residual risk remains largely unchanged and no action by management or the Internal Audit Department is planned, the Director of Internal Audit will report those areas separately to the Audit Committee with details of the risk analysis and reasons for the lack of, or ineffectiveness of, internal controls.

A selection of lower risk level business unit or branch type audits will periodically be included in the Internal Audit Department's plan to give them coverage and confirm that their risks have not changed. Also, the Internal Audit Department establishes a method for prioritizing outstanding risks not yet subject to an internal audit.

The Internal Audit Department's plan focuses on:

- Unacceptable current risks where management action is required. These would be areas with minimal key controls or mitigating factors that senior management wants audited immediately.
- Control systems on which the University is most reliant.
- Areas where the differential is great between inherent risk and residual risk.
- Areas where the inherent risk is very high.
- When planning individual internal audits, the internal auditor identifies and assesses risks relevant to the area under review

Communication and Approval

The Director of Internal Audit will communicate the Internal Audit Department's plans and resource requirements, including significant interim changes, to senior management and the Audit Committee for review and approval. The Director of Internal Audit will also communicate the impact of resource limitations.

The Director of Internal Audit will submit annually to senior management and the Audit Committee for review and approval a summary of the internal audit plan, work schedule, staffing plan, and financial budget. This summary will inform senior management and the Audit Committee of the scope of internal audit work and of any limitations placed on that scope. The Director of Internal Audit will also submit all significant interim changes for approval and information.

The approved engagement work schedule, staffing plan, and financial budget, along with all significant interim changes, are to contain sufficient information to enable senior management and the Audit Committee to ascertain whether the Internal Audit Department's objectives and plans support those of the University and the Audit Committee and are consistent with the Internal Audit Charter.

Resource Management

The Director of Internal Audit will ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan.

Resources are effectively deployed when they are used in a way that optimizes the achievement of the approved plan.

The Director of Internal Audit is primarily responsible for the sufficiency and management of internal audit resources in a manner that ensures the fulfillment of internal audit's responsibilities, as detailed in the Internal Audit Charter. This includes effective communication of resource needs and reporting of status to senior management and the Audit Committee. Internal audit resources will include employees, external service providers, financial support, and technology-based audit techniques. Ensuring the adequacy of Internal Audit resources is ultimately a responsibility of the University's senior management and Audit Committee; the Director of Internal Audit will assist them in discharging this responsibility.

The skills, capabilities, and technical knowledge of the internal audit staff are to be appropriate for the planned activities. The Director of Internal Audit will conduct a periodic skills assessment or inventory to determine the specific skills required to perform the Internal Audit activities. The skills assessment is based on and considers the various needs identified in the risk assessment and audit plan. This includes assessments of technical knowledge, business acumen, fraud detection and prevention competency, and accounting and audit expertise.

Internal audit resources need to be sufficient to execute the audit activities in the breadth, depth, and timeliness expected by senior management and the Audit Committee, as stated in the Internal Audit Charter. Resource planning considerations

include the audit universe, relevant risk levels, the internal audit plan, coverage expectations, and an estimate of unanticipated activities.

The Director of Internal Audit also ensures that resources are deployed effectively. This includes assigning auditors who are competent and qualified for specific assignments. It also includes developing a resourcing approach and organizational structure appropriate for the business structure and risk profile of the University.

From an overall resource management standpoint, the Director of Internal Audit considers succession planning, staff evaluation and development programs, and other human resource disciplines. The Director of Internal Audit also addresses the resourcing needs of the Internal Audit Department, whether those skills are present or not within the Internal Audit Department itself. Other approaches to addressing resource needs include external service providers, employees from other departments within the University, or specialized consultants.

Because of the critical nature of resources, the Director of Internal Audit maintains ongoing communications and dialog with senior management and the Audit Committee on the adequacy of resources for the Internal Audit Department. The Director of Internal Audit periodically presents a summary of status and adequacy of resources to senior management and the Audit Committee. To that end, the Director of Internal Audit develops appropriate metrics, goals, and objectives to monitor the overall adequacy of resources. This can include comparisons of resources to the internal audit plan, the impact of temporary shortages or vacancies, educational and training activities, and changes to specific skill needs based on changes in the University's business, operations, programs, systems, and controls.

Policies and Procedures

The Director of Internal Audit has established these policies and procedures to guide the Internal Audit Department.

The Director of Internal Audit developed these policies and procedures. Formal administrative and technical audit manuals will be developed by the Internal Audit Department as needed. The Audit staff is also directed and controlled through daily, close supervision and memoranda that state policies and procedures to be followed. Formal and comprehensive policies and procedures are essential to guide the Internal Audit staff in the execution of the Internal Audit plan.

Coordination

The Director of Internal Audit will share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

Oversight of the work of external auditors, including coordination with the Internal Audit Department, is the responsibility of the Audit Committee. Coordination of internal and external audit work is the responsibility of the Director of Internal Audit. The Director of Internal Audit will obtain the support of the Audit Committee to coordinate audit work effectively.

The University may use the work of external auditors to provide assurance related to activities within the scope of internal auditing. In these cases, the Director of Internal Audit will take the steps necessary to understand the work performed by the external auditors, including:

- The nature, extent, and timing of work planned by external auditors, to be satisfied that the external auditors' planned work, in conjunction with the internal auditors' planned work, is satisfactory.
- The external auditor's assessment of risk and materiality.
- The external auditors' techniques, methods, and terminology to enable the Director of Internal Audit to (1) coordinate internal and external auditing work; (2) evaluate, for purposes of reliance, the external auditors' work; and (3) communicate effectively with external auditors.
- Access to the external auditors' programs and working papers, to be satisfied that the external auditors' work can be relied upon for internal audit purposes. Internal auditors are responsible for respecting the confidentiality of those programs and working papers.

The external auditor may rely on the work of the Internal Audit Department in performing their work. In this case, the Director of Internal Audit will provide sufficient information to enable external auditors to understand the internal auditors' techniques, methods, and terminology to facilitate reliance by external auditors on work performed. Access to the internal auditors' programs and working papers is provided to external auditors in order for external auditors to be satisfied as to the acceptability for external audit purposes of relying on the internal auditors' work.

It may be efficient for internal and external auditors to use similar techniques, methods, and terminology to coordinate their work effectively and to rely on the work of one another.

Planned audit activities of internal and external auditors will be discussed to ensure that audit coverage is coordinated and duplicate efforts are minimized where possible.

Sufficient meetings will be scheduled during the audit process to ensure coordination of audit work and efficient and timely completion of audit activities, and to determine whether observations and recommendations from work performed to date require that the scope of planned work be adjusted.

The Internal Audit Department's final communications, management's responses to those communications, and subsequent follow-up reviews are to be made available to external auditors. These communications assist external auditors in determining and adjusting the scope and timing of their work. In addition, internal auditors need access to the external auditors' presentation materials and management letters. Matters discussed in presentation materials and included in management letters need to be understood by the Director of Internal Audit and used as input to internal auditors in planning the areas to emphasize in future internal audit work.

After review of management letters and initiation of any needed corrective action by appropriate members of senior management and the Audit Committee, the Director of Internal Audit ensures that appropriate follow-up and corrective actions have been taken.

The Director of Internal Audit is responsible for regular evaluations of the coordination between internal and external auditors. Such evaluations will also include assessments of the overall efficiency and effectiveness of internal and external audit activities, including aggregate audit cost.

The Director of Internal Audit communicates the results of these evaluations to senior management and the Audit Committee, including relevant comments about the performance of external auditors.

Assurance Maps

The Director of Internal Audit will share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

One of the key responsibilities of the Audit Committee is to gain assurance that processes are operating within the parameters it has established to achieve the defined

objectives. It is necessary to determine whether risk management processes are working effectively and whether key or business-critical risks are being managed to an acceptable level.

Increased focus on the roles and responsibilities of senior management and audit committees has prompted many universities to place a greater emphasis on assurance activities. The glossary in the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* defines assurance as "an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization." The Audit Committee will use multiple sources to gain reliable assurance. Assurance from management is fundamental and should be complemented by the provision of objective assurance from Internal Audit and other third parties. Risk managers, internal auditors, and compliance practitioners are asking: "Who does what and why?" Audit Committees in particular are beginning to question who is providing assurance, where is the delineation between the functions, and if there are any overlaps.

There are fundamentally three classes of assurance providers, differentiated by the stakeholders they serve, their level of independence from the activities over which they provide assurance, and the robustness of that assurance.

- Those who report to management and/or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors, and other management- designated assurance personnel.
- Those who report to the Audit Committee, including Internal Audit.
- Those who report to external stakeholders (external audit assurance), which is a role traditionally fulfilled by the independent/statutory auditor.

The level of assurance desired, and who should provide that assurance, will vary depending on the risk.

There are many assurance providers for the University.

- Line management and employees (management provides assurance as a first line of defense over the risks and controls for which they are responsible.)
- Senior management
- Internal and external auditors
- Compliance
- Quality assurance

- Risk management
- Environmental auditors
- Workplace health and safety auditors
- Government performance auditors
- Financial reporting review teams
- Subcommittees of the Board of Trustees (e.g., Audit, Governance)
- External assurance providers, including surveys, specialist reviews (health and safety), etc.

The Internal Audit Department will normally provide assurance over the entire University, including risk management processes (both their design and operating effectiveness), management of those risks classified as “key” (including the effectiveness of the controls and other responses to them), verification of the reliability and appropriateness of the risk assessment and reporting of the risk and control status.

With responsibility for assurance activities traditionally being shared among management, Internal Audit, risk management, and compliance, it is important that assurance activities be coordinated to ensure resources are used in the most efficient and effective way. Many universities operate with traditional (and separate) internal audit, risk, and compliance activities. It is common for universities to have a number of separate groups performing different risk management, compliance, and assurance functions independently of one another. Without effective coordination and reporting, work can be duplicated or key risks may be missed or misjudged.

While many universities monitor the activities of Internal Audit, risk, and compliance, not all view all their activities in a holistic way. An assurance mapping exercise involves mapping assurance coverage against the key risks in the University. This process allows the University to identify and address any gaps in the risk management process and gives stakeholders comfort that risks are being managed and reported on, and that regulatory and legal obligations are being met. Universities benefit from a streamlined approach, which ensures the information is available to management about the risks they face and how the risks are being addressed. The mapping is done across the University to understand where the overall risk and assurance roles and accountabilities reside. The aim is to ensure that there is a comprehensive risk and assurance process with no duplicated effort or potential gaps.

The University has defined the significant risk categories that make up its risk management framework. The assurance map will be based on the structure of this framework. An assurance map will have these columns:

- Significant risk category
- Management role responsible for the risk (risk owner)
- Inherent risk rating
- Residual risk rating
- External audit coverage
- Internal audit coverage
- Other assurance provider coverage

The Director of Internal Audit will populate the internal audit coverage column with recent coverage. Often each significant risk has a risk owner or a person responsible for coordinating assurance activities for that risk and that person would populate the other assurance provider coverage column. Each significant unit within the University will have its own assurance map. Alternatively, the Internal Audit Department will play a coordinating role in developing and completing the University's assurance map.

Once the assurance map for the University has been completed, significant risks with inadequate assurance coverage, or areas of duplicated assurance coverage, can be identified. Senior management and the Audit Committee will consider changes in assurance coverage for these risks. The Internal Audit Department will consider areas of inadequate coverage when developing the Internal Audit plan.

It is the responsibility of the Director of Internal Audit to understand the independent assurance requirements of the Audit Committee and the University, to clarify the role the Internal Audit Department fills and the level of assurance it provides. The Audit Committee will be confident that the overall assurance process is adequate and sufficiently robust to validate that the risks of the University are being managed and reported on effectively.

The Audit Committee will receive information about assurance activities, both implemented and planned, in regard to each category of risk. The Internal Audit Department and other assurance providers offer the Audit Committee the appropriate level of assurance for the nature and levels of risk that exist in the University under the respective categories.

The Director of Internal Audit will understand the nature, scope, and extent of the integrated assurance map to consider the work of other assurance providers (and rely on it as appropriate) before presenting an overall opinion on the University's governance, risk management, and control processes. The IIA's Practice Guide *Formulating and Expressing Internal Audit Opinions* provides additional guidance.

The Director of Internal Audit will coordinate activities with other assurance providers; the use of an assurance map will help achieve this. Assurance maps increasingly offer an effective way of communicating this coordination.

Reporting to Senior Management and the Audit Committee

The Director of Internal Audit will report periodically to senior management and the Audit Committee on the Internal Audit Department's purpose, authority, responsibility, and performance relative to its plan.

Reporting will also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the Audit Committee.

The frequency and content of reporting are determined in discussion with senior management and the Audit Committee and depend on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management or the Audit Committee.

The Director of Internal Audit will submit activity reports to senior management and the Audit Committee periodically. Activity reports highlight significant engagement observations and recommendations and inform senior management and the Audit Committee of significant deviations from approved engagement work schedules, staffing plans, and financial budgets; the reasons for the deviations; and action taken or needed.

Significant engagement observations are those conditions that, in the judgment of the Director of Internal Audit, could adversely affect the University. Significant engagement observations include conditions dealing with fraud, irregularities, illegal acts, errors, inefficiency, waste, ineffectiveness, conflicts of interest, and control weaknesses.

Senior management and the Audit Committee make decisions on the appropriate action to be taken regarding significant engagement observations and recommendations.

Senior management and the Audit Committee may decide to assume the risk of not correcting the reported condition because of cost or other considerations. The Audit Committee will be informed of senior management's decisions on all significant engagement observations and recommendations.

The Director of Internal Audit considers whether it is appropriate to inform the Audit Committee regarding previously reported, significant engagement observations and recommendations in those instances when senior management and the Audit Committee assumed the risk of not correcting the reported condition. This will be necessary when there have been significant changes that affect the risk profile.

Assessing the Adequacy of Risk Management Processes

The Internal Audit Department must evaluate the effectiveness and contribute to the improvement of risk management processes.

Determining whether risk management processes are effective is a judgment resulting from internal auditor's assessment that:

- University objectives support and align with the University's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the University's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the University, enabling staff, management, and the Audit Committee to carry out their responsibilities.
- Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

Risk management is a key responsibility of senior management and the Audit Committee. To achieve its business objectives, management ensures that sound risk management processes are in place and functioning. The Audit Committee has an oversight role to determine that appropriate risk management processes are in place and that these processes are adequate and effective.

In this role, they direct the Internal Audit Department to assist them by examining, evaluating, reporting, and/or recommending improvements to the adequacy and effectiveness of management's risk processes.

Management and the Audit Committee are responsible for the University's risk management and control processes. However, internal auditors acting in a consulting role can assist the University in identifying, evaluating, and implementing risk management methodologies and controls to address those risks.

The Director of Internal Audit will formally discuss with management and the Audit Committee their obligations to understand, manage, and monitor risks within the University and the need to satisfy themselves that there are processes operating within the University, even if informal, that provide the appropriate level of visibility into the key risks and how they are being managed and monitored.

The Director of Internal Audit will obtain an understanding of senior management's and the Audit Committee's expectations of the Internal Audit Department in the University's risk management process.

This understanding is then codified in the Charters of the Internal Audit Department and the Audit Committee. Internal Audit's responsibilities are coordinated between all groups and individuals within the University's risk management process. The Internal Audit Department's role in the risk management process of the University can change over time and may encompass:

- No role.
- Auditing the risk management process as part of the internal audit plan.
- Active, continuous support and involvement in the risk management process such as participation on oversight committees, monitoring activities, and status reporting.
- Managing and coordinating the risk management process.

Ultimately, it is the role of senior management and the Audit Committee to determine the role of internal auditing in the risk management process. Their view on Internal Audit's role is likely to be determined by factors such as the culture of the University and ability of the Internal Audit staff. However, taking on management's responsibility regarding the risk management process and the potential threat to the Internal Audit Department's independence requires a full discussion and Audit Committee approval.

The techniques used by the University for its Risk Management Practices can be:

- Formal or informal.
- Quantitative or subjective.
- Embedded in the business units or centralized at a University level.

The University designs processes based on its culture, management style, and business objectives. For example, the use of derivatives or other sophisticated capital

markets products by the University could require the use of quantitative risk management tools.

The internal auditor determines that the methodology chosen is sufficiently comprehensive and appropriate for the nature of the University's activities.

The internal auditors will obtain sufficient and appropriate evidence to determine that the key objectives of the risk management processes are being met to form an opinion on the adequacy of risk management processes. In gathering such evidence, the internal auditor might consider the following audit procedures:

- Research and review current developments, trends, industry information related to the business conducted by the University, and other appropriate sources of information to determine risks and exposures that will affect the University and related control procedures used to address, monitor, and reassess those risks.
- Review University policies and Board of Trustee minutes to determine the University's business strategies, risk management philosophy and methodology, appetite for risk, and acceptance of risks.
- Review previous risk evaluation reports issued by management, internal auditors, external auditors, and any other sources.
- Conduct interviews with line and senior management to determine business unit objectives, related risks, and management's risk mitigation and control monitoring activities.
- Assimilate information to independently evaluate the effectiveness of risk mitigation, monitoring, and communication of risks and associated control activities.
- Assess the appropriateness of reporting lines for risk monitoring activities.
- Review the adequacy and timeliness of reporting on risk management results.
- Review the completeness of management's risk analysis and actions taken to remedy issues raised by risk management processes, and suggest improvements.
- Determine the effectiveness of management's self-assessment processes through observations, direct tests of control and monitoring procedures, testing the accuracy of information used in monitoring activities, and other appropriate techniques.
- Review risk-related issues that may indicate weakness in risk management practices and, as appropriate, discuss with senior management and the Audit Committee.

Assessing the Adequacy of Control Processes

The Internal Audit Department will assist the University in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

The University establishes and maintains effective risk management and control processes. The purpose of control processes is to support the University in the management of risks and the achievement of its established and communicated objectives.

The control processes are expected to ensure, among other things, that:

- Financial and operational information is reliable and possesses integrity,
- Operations are performed efficiently and achieve established objectives,
- Assets are safeguarded, and
- Actions and decisions of the University are in compliance with laws, regulations, and contracts.

Senior management's role is to oversee the establishment, administration, and assessment of the system of risk management and control processes. Among the responsibilities of the University's line managers is the assessment of the control processes in their respective areas. Internal auditors provide varying degrees of assurance about the effectiveness of the risk management and control processes in select activities and functions of the University.

The Director of Internal Audit forms an overall opinion about the adequacy and effectiveness of the control processes. The expression of such an opinion by the Director of Internal Audit will be based on sufficient audit evidence obtained through the completion of audits and, where appropriate, reliance on the work of other assurance providers. The Director of Internal Audit communicates the opinion to senior management and the Audit Committee.

The Director of Internal Audit develops a proposed internal audit plan to obtain sufficient evidence to evaluate the effectiveness of the control processes. The plan includes audit engagements and/or other procedures to obtain sufficient, appropriate audit evidence about all major operating units and business functions to be assessed, as well as a review of the major control processes operating across the University. The plan should be flexible so that adjustments may be made during the year as a result of changes in management strategies, external conditions, major risk areas, or revised expectations about achieving the University's objectives.

The audit plan gives special consideration to those operations most affected by recent or unexpected changes. Changes in circumstances can result, for example, from marketplace or investment conditions, acquisitions and divestitures, University restructuring, new systems, and new ventures.

In determining the expected audit coverage for the proposed audit plan, the Director of Internal Audit considers relevant work performed by others who provide assurances to senior management (e.g., reliance by the Director of Internal Audit on the work of University compliance officers). The Director of Internal Audit's audit plan also considers audit work completed by the external auditor and management's own assessments of its risk management process, controls, and quality improvement processes.

The Director of Internal Audit should evaluate the breadth of coverage of the proposed audit plan to determine whether the scope is sufficient to enable the expression of an opinion about the University's risk management and control processes. The Director of Internal Audit should inform senior management and the Audit Committee of any gaps in audit coverage that would prevent the expression of an opinion on all aspects of these processes.

A key challenge for the Internal Audit Department is to evaluate the effectiveness of the University's control processes based on the aggregation of many individual assessments.

Those assessments are largely gained from internal audit engagements, reviews of management's self-assessments, and other assurance providers' work. As the engagements progress, internal auditors communicate, on a timely basis, the findings to the appropriate levels of management so prompt action can be taken to correct or mitigate the consequences of discovered control discrepancies or weaknesses.

In evaluating the overall effectiveness of the University's control processes, the Director of Internal Audit considers whether:

- Significant discrepancies or weaknesses were discovered,
- Corrections or improvements were made after the discoveries, and
- The discoveries and their potential consequences lead to a conclusion that a pervasive condition exists resulting in an unacceptable level of risk.

The existence of a significant discrepancy or weakness does not necessarily lead to the judgment that it is pervasive and poses an unacceptable risk. The internal auditor considers the nature and extent of risk exposure, as well as the level of potential

consequences in determining whether the effectiveness of the control processes are jeopardized and unacceptable risks exist.

The Director of Internal Audit's report on the University's control processes is normally presented once a year to senior management and the Audit Committee. The report states the critical role played by the control processes in the achievement of the University's objectives. The report also describes the nature and extent of the work performed by the Internal Audit Department and the nature and extent of reliance on other assurance providers in formulating the opinion.

Information Reliability and Integrity

The Internal Audit Department will evaluate the adequacy and effectiveness of controls in responding to the risks within the University's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

The internal auditors determine whether senior management and the Audit Committee have a clear understanding that information reliability and integrity is a management responsibility. This responsibility includes all critical information of the University regardless of how the information is stored. Information reliability and integrity includes accuracy, completeness, and security.

The Director of Internal Audit determines whether the Internal Audit Department possesses, or has access to, competent audit resources to evaluate information reliability and integrity and associated risk exposures. This includes both internal and external risk exposures, and exposures relating to the University's relationships with outside entities.

The Director of Internal Audit determines whether information reliability and integrity breaches and conditions that might represent a threat to the University will promptly be made known to senior management, the Audit Committee, and the Internal Audit Department.

The internal auditors assess the effectiveness of preventive, detective, and mitigation measures against past attacks, as appropriate, and future attempts or incidents deemed likely to occur.

The internal auditors determine whether the Audit Committee has been appropriately informed of threats, incidents, vulnerabilities exploited, and corrective measures.

The internal auditors periodically assess the University's information reliability and integrity practices and recommend, as appropriate, enhancements to, or implementation of, new controls and safeguards. Such assessments can either be conducted as separate standalone engagements or integrated into other audits or engagements conducted as part of the Internal Audit Plan. The nature of the engagement will determine the most appropriate reporting process to senior management and the Audit Committee.

Evaluating the University's Privacy Framework

The Internal Audit Department will evaluate the adequacy and effectiveness of controls in responding to the risks within the University's governance, operations, and information systems regarding the:

- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, and contracts.

The failure to protect personal information with appropriate controls can have significant consequences for the University. The failure could damage the reputation of individuals and/or the University, and expose the University to risks that include legal liability and diminished consumer and/or employee trust.

Risks associated with the privacy of information encompass personal privacy (physical and psychological); privacy of space (freedom from surveillance); privacy of communication (freedom from monitoring); and privacy of information (collection, use, and disclosure of personal information by others). Personal information generally refers to information associated with a specific individual, or that has identifying characteristics that, when combined with other information, can then be associated with a specific individual. It can include any factual or subjective information — recorded or not — in any form of media. Personal information could include:

- Name, address, identification numbers, family relationships;
- Employee files, evaluations, comments, social status, or disciplinary actions;
- Credit records, income, financial status, or
- Medical status.

Effective control over the protection of personal information is an essential component of the governance, risk management, and control processes of the University. The Audit Committee is ultimately accountable for identifying the principal risks to the University and implementing appropriate control processes to mitigate those risks. This includes establishing the necessary privacy framework for the University and monitoring its implementation.

The Internal Audit Department can contribute to good governance and risk management by assessing the adequacy of management's identification of risks related to its privacy objectives and the adequacy of the controls established to mitigate those risks to an acceptable level. The internal auditor is well positioned to evaluate the privacy framework in the University and identify the significant risks, as well as the appropriate recommendations for mitigation.

The Internal Audit Department identifies the types and appropriateness of information gathered by the University that is deemed personal or private, the collection methodology used, and whether the University's use of that information is in accordance with its intended use and applicable legislation.

Given the highly technical and legal nature of privacy issues, the Internal Audit Department needs appropriate knowledge and competence to conduct an assessment of the risks and controls of the University's privacy framework.

In conducting such an evaluation of the management of the University's privacy framework, the internal auditor:

- Considers the laws, regulations, and policies relating to privacy in the jurisdictions where the University operates;
- Liaisons with in-house legal counsel to determine the exact nature of laws, regulations, and other standards and practices applicable to the University;
- Liaisons with information technology specialists to determine that information security and data protection controls are in place and regularly reviewed and assessed for appropriateness;
- Considers the level or maturity of the University's privacy practices. Depending upon the level, the internal auditor may have differing roles. The auditor may

facilitate the development and implementation of the privacy program, evaluate management's privacy risk assessment to determine the needs and risk exposures of the University, or provide assurance on the effectiveness of the privacy policies, practices, and controls across the University. If the internal auditor assumes any responsibility for developing and implementing a privacy program, the internal auditor's independence will be impaired.

Engagement Planning

The internal auditors will develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

The internal auditor plans and conducts the engagement, with supervisory review and approval. Prior to the engagement's commencement, the internal auditor prepares an engagement program that:

- States the objectives of the engagement.
- Identifies technical requirements, objectives, risks, processes, and transactions that are to be examined.
- States the nature and extent of testing required.
- Documents the internal auditor's procedures for collecting, analyzing, interpreting, and documenting information during the engagement.
- Is modified, as appropriate, during the engagement with the approval of the Director of Internal Audit, or his or her designee.

The Director of Internal Audit will require a level of formality and documentation (e.g., of the results of planning meetings, risk assessment procedures, level of detail in the work program, etc.) that is appropriate to the University. Factors to consider include:

- Whether the work performed and/or the results of the engagement will be relied upon by others (e.g., external auditors, regulators, or management).
- Whether the work relates to matters that may be involved in potential or current litigation.
- The experience level of the Internal Audit staff and the level of direct supervision required.
- Whether the project is staffed internally, by guest auditors, or by external service providers.
- The project's complexity and scope.
- The size of the Internal Audit Department.

- The value of documentation (e.g., whether it will be used in subsequent years).

The internal auditor determines the other engagement requirements, such as the period covered and estimated completion dates. The internal auditor also considers the final engagement communication format. Planning at this stage facilitates the communication process at the engagement's completion.

The internal auditor informs those in management who need to know about the engagement, conducts meetings with management responsible for the activity under review, summarizes and distributes the discussions and any conclusions reached from the meetings, and retains the documentation in the engagement working papers. Topics of discussion may include:

- Planned engagement objectives and scope of work.
- The resources and timing of engagement work.
- Key factors affecting business conditions and operations of the areas being reviewed, including recent changes in internal and external environment.
- Concerns or requests from management.

The Director of Internal Audit determines how, when, and to whom engagement results will be communicated.

The internal auditor documents this and communicates it to management, to the extent deemed appropriate, during the planning phase of the engagement. The internal auditor communicates to management subsequent changes that affect the timing or reporting of engagement results.

Engagement Objectives

Objectives must be established for each engagement.

The internal auditors establish engagement objectives to address the risks associated with the activity under review. For planned engagements, the objectives proceed and align to those initially identified during the risk assessment process from which the Internal Audit Plan is derived. For unplanned engagements, the objectives are established prior to the start of the engagement and are designed to address the specific issue that prompted the engagement.

The risk assessment during the engagement's planning phase is used to further define the initial objectives and identify other significant areas of concern.

After identifying the risks, the auditor determines the procedures to be performed and the scope (nature, timing, and extent) of those procedures. Engagement procedures performed in appropriate scope are the means to derive conclusions related to the engagement objectives.

Risk Assessment in Engagement Planning

The 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.

The internal auditors consider management's assessment of risks relevant to the activity under review. The internal auditor also considers:

- The reliability of management's assessment of risk.
- Management's process for monitoring, reporting, and resolving risk and control issues.
- Management's reporting of events that exceeded the limits of the University's risk appetite and management's response to those reports.
- Risks in related activities relevant to the activity under review.

The internal auditors obtain or update background information about the activities to be reviewed to determine the impact on the engagement objectives and scope.

If appropriate, internal auditors conduct a survey to become familiar with the activities, risks, and controls to identify areas for engagement emphasis, and to invite comments and suggestions from engagement clients.

The internal auditors summarize the results from the reviews of management's assessment of risk, the background information, and any survey work. The summary includes:

- Significant engagement issues and reasons for pursuing them in more depth.
- Engagement objectives and procedures.
- Methodologies to be used, such as technology-based audit and sampling techniques.
- Potential critical control points, control deficiencies, and/or excess controls.

- When applicable, reasons for not continuing the engagement or for significantly modifying engagement objectives.

Engagement Resource Allocation

The internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

The internal auditors consider the following when determining the appropriateness and sufficiency of resources:

- The number and experience level of the Internal Audit staff.
- Knowledge, skills, and other competencies of the Internal Audit staff when selecting internal auditors for the engagement.
- Availability of external resources where additional knowledge and competencies are required.
- Training needs of internal auditors as each engagement assignment serves as a basis for meeting the Internal Audit Department's developmental needs.

Engagement Work Program

The internal auditors must develop and document work programs that achieve the engagement objectives.

The internal auditors will develop and obtain documented approval of work programs before commencing the internal audit engagement. The work program includes methodologies to be used, such as technology-based audit and sampling techniques.

The process of collecting, analyzing, interpreting, and documenting information is to be supervised to provide reasonable assurance that engagement objectives are met and that the internal auditor's objectivity is maintained.

Documenting Information

Internal auditors must document relevant information to support the conclusions and engagement results.

The internal auditors prepare working papers. Working papers document the information obtained, the analyses made, and the support for the conclusions and engagement results.

Internal audit management reviews the prepared working papers.

Engagement working papers generally:

- Aid in the planning, performance, and review of engagements.
- Provide the principal support for engagement results.
- Document whether engagement objectives were achieved.
- Support the accuracy and completeness of the work performed.
- Provide a basis for the Internal Audit Department's quality assurance and improvement program.
- Facilitate third-party reviews.

The organization, design, and content of engagement working papers depend on the engagement's nature and objectives and the University's needs. Engagement working papers document all aspects of the engagement process from planning to communicating results. The Internal Audit Department determines the media used to document and store working papers.

The Director of Internal Audit establishes working paper policies for the various types of engagements performed. Standardized engagement working papers, such as questionnaires and audit programs, may improve the engagement's efficiency and facilitate the delegation of engagement work. Engagement working papers will be categorized as permanent or carry-forward engagement files that contain information of continuing importance.

Control of Engagement Records

The Director of Internal Audit will control access to engagement records. The Director of Internal Audit must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.

Internal audit engagement records include reports, supporting documentation, review notes, and correspondence, regardless of storage media. Engagement records or working papers are the property of the University. The Internal Audit Department controls engagement working papers and provides access to authorized personnel only.

The internal auditors will educate management and the Audit Committee about access to engagement records by external parties. Policies relating to access to engagement records, handling of access requests, and procedures to be followed when an engagement warrants an investigation, will be reviewed by the Audit Committee.

Internal Audit policies explain who in the University is responsible for ensuring the control and security of the Department's records; which internal or external parties can be granted access to engagement records; and how requests for access to those records need to be handled.

Management and other members of the University may request access to all or specific engagement working papers. Such access will be necessary to substantiate or explain engagement observations and recommendations or for other business purposes. The Director of Internal Audit approves these requests.

The Director of Internal Audit will approve access to engagement working papers by external auditors.

There are circumstances where parties outside the University, other than external auditors, request access to engagement working papers and reports. Prior to releasing the documentation, the Director of Internal Audit will obtain the approval of senior management and/or legal counsel, as appropriate.

Potentially, Internal Audit records that are not specifically protected may be accessed in legal proceedings. Legal requirements vary significantly in different jurisdictions. When there is a specific request for engagement records in relation to a legal proceeding, the Director of Internal Audit will work closely with legal counsel in deciding what to provide.

Retention of Records

The Director of Internal Audit has developed retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the University's guidelines and any pertinent regulatory or other requirements.

The Director of Internal Audit will develop a written retention policy that meets University needs and legal requirements of the jurisdictions within which the University operates.

The record retention policy includes appropriate arrangements for the retention of records related to engagements performed by external service providers.

Engagement Supervision

Engagements will be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

The extent of supervision required will depend on the proficiency and experience of the internal auditors and the complexity of the engagement. The Director of Internal Audit has overall responsibility for supervising the engagement, whether performed by or for the Internal Audit Department, but may designate appropriately experienced members of the Internal Audit Department to perform the review. Appropriate evidence of supervision is documented and retained.

The Director of Internal Audit or designee provides appropriate engagement supervision.

Supervision is a process that begins with planning and continues throughout the engagement. The process includes:

- Ensuring designated auditors collectively possess the required knowledge, skills, and other competencies to perform the engagement.
- Providing appropriate instructions during the planning of the engagement and approving the engagement program.
- Ensuring the approved engagement program is completed unless changes are justified and authorized.
- Determining engagement working papers adequately support engagement observations, conclusions, and recommendations.
- Ensuring engagement communications are accurate, objective, clear, concise, constructive, and timely.
- Ensuring engagement objectives are met.
- Providing opportunities for developing internal auditors' knowledge, skills, and other competencies.

The Director of Internal Audit is responsible for all internal audit engagements, whether performed by or for the Internal Audit Department, and all significant professional judgments made throughout the engagement. The Director of Internal Audit will also adopt suitable means to ensure this responsibility is met.

Suitable means include policies and procedures designed to resolve differences in professional judgment between the Director of Internal Audit and internal audit staff over significant issues relating to the engagement. Such means will include discussion of pertinent facts, further inquiry or research, and documentation and disposition of the differing viewpoints in engagement working papers. In instances of a difference in professional judgment over an ethical issue, suitable means may include referral of the issue to those individuals in the University having responsibility over ethical matters.

All engagement working papers are reviewed to ensure they support engagement communications and necessary audit procedures are performed. Evidence of supervisory review consists of the reviewer initialing and dating each working paper after it is reviewed.

Other techniques that provide evidence of supervisory review include completing an engagement working paper review checklist; preparing a memorandum specifying the nature, extent, and results of the review; or evaluating and accepting reviews within the working paper software.

Reviewers can make a written record (i.e., review notes) of questions arising from the review process. When clearing review notes, care will be taken to ensure working papers provide adequate evidence that questions raised during the review are resolved.

Alternatives with respect to disposition of review notes are as follows:

- Retain the review notes as a record of the reviewer's questions raised, the steps taken in their resolution, and the results of those steps.
- Discard the review notes after the questions raised are resolved and the appropriate engagement working papers are amended to provide the information requested.

Engagement supervision also allows for training and development of staff and performance evaluation.

Communication Criteria

Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

Although the format and content of the final engagement communications varies by type of engagement, they are to contain, at a minimum, the purpose, scope, and results of the engagement.

Final engagement communications may include background information and summaries.

Background information may identify the organizational units and activities reviewed and provide explanatory information. It may also include the status of observations, conclusions, and recommendations from prior reports and an indication of whether the report covers a scheduled engagement or is responding to a request. Summaries are balanced representations of the communication's content.

Purpose statements describe the engagement objectives and will inform the reader why the engagement was conducted and what it was expected to achieve.

Scope statements identify the audited activities and may include supportive information such as time period reviewed and related activities not reviewed to delineate the boundaries of the engagement. They will describe the nature and extent of engagement work performed.

Results include observations, conclusions, opinions, recommendations, and action plans.

Observations are pertinent statements of fact. The internal auditor communicates those observations necessary to support or prevent misunderstanding of the internal auditor's conclusions and recommendations. The internal auditor may communicate less significant observations or recommendations informally.

Engagement observations and recommendations emerge by a process of comparing criteria (the correct state) with condition (the current state). Whether or not there is a difference, the internal auditor has a foundation on which to build the report. When conditions meet the criteria, communication of satisfactory performance may be appropriate. Observations and recommendations are based on the following attributes:

- Criteria: The standards, measures, or expectations used in making an evaluation and/or verification (the correct state).
- Condition: The factual evidence that the internal auditor found in the course of the examination (the current state).
- Cause: The reason for the difference between expected and actual conditions.

- Effect: The risk or exposure the University and/or others encounter because the condition is not consistent with the criteria (the impact of the difference). In determining the degree of risk or exposure, internal auditors consider the effect their engagement observations and recommendations may have on the University's operations and financial statements.

Observations and recommendations can include engagement client accomplishments, related issues, and supportive information.

Conclusions and opinions are the internal auditor's evaluations of the effects of the observations and recommendations on the activities reviewed. They usually put the observations and recommendations in perspective based upon their overall implications.

Clearly identify any engagement conclusions in the engagement report. Conclusions will encompass the entire scope of an engagement or specific aspects. They may cover, but are not limited to, whether operating or program objectives and goals conform to those of the University, whether the University's objectives and goals are being met, and whether the activity under review is functioning as intended. An opinion may include an overall assessment of controls or may be limited to specific controls or aspects of the engagement.

The internal auditor will communicate recommendations for improvements, acknowledgments of satisfactory performance, and corrective actions.

Recommendations are based on the internal auditor's observations and conclusions.

They call for action to correct existing conditions or improve operations and may suggest approaches to correcting or enhancing performance as a guide for management in achieving desired results.

Recommendations can be general or specific. For example, under some circumstances, the internal auditor may recommend a general course of action and specific suggestions for implementation. In other circumstances, the internal auditor may suggest further investigation or study.

The internal auditor may communicate engagement client accomplishments, in terms of improvements since the last engagement or the establishment of a well-controlled operation.

The internal auditor will communicate the engagement client's views about the internal auditor's conclusions, opinions, or recommendations.

As part of the internal auditor's discussions with the engagement client, the internal auditor obtains agreement on the results of the engagement and on any necessary plan of action to improve operations. If the internal auditor and engagement client disagree about the engagement results, the engagement communications state both positions and the reasons for the disagreement. The engagement client's written comments may be included as an appendix to the engagement report, in the body of the report, or in a cover letter.

Certain information is not appropriate for disclosure to all report recipients because it is privileged, proprietary, or related to improper or illegal acts. Disclose such information in a separate report. Distribute the report to the Audit Committee if the conditions being reported involve senior management.

Interim reports are written or oral and may be transmitted formally or informally. Use interim reports to communicate information that requires immediate attention, to communicate a change in engagement scope for the activity under review, or to keep management informed of engagement progress when engagements extend over a long period. The use of interim reports does not diminish or eliminate the need for a final report.

A signed report is issued after the engagement's completion. Summary reports highlighting engagement results are appropriate for levels of management above the engagement client and can be issued separately from or in conjunction with the final report. The term "signed" means the authorized internal auditor's name is manually or electronically signed in the report or on a cover letter. The Director of Internal Audit will determine which internal auditor is authorized to sign the report. When engagement reports are distributed by electronic means, a signed version of the report is kept on file by the Internal Audit Department.

Quality of Communications

Communications will be accurate, objective, clear, concise, constructive, complete, and timely.

Accurate communications are free from errors and distortions and are faithful to the underlying facts. Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and

circumstances. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness. Constructive communications are helpful to the engagement client and the University and lead to improvements where needed. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

Gather, evaluate, and summarize data and evidence with care and precision.

Derive and express observations, conclusions, and recommendations without prejudice, partisanship, personal interests, and the undue influence of others.

Improve clarity by avoiding unnecessary technical language and providing all significant and relevant information in context.

Develop communications with the objective of making each element meaningful but succinct.

Adopt a useful, positive, and well-meaning content and tone that focuses on the University's objectives.

Ensure communication is consistent with the University's style and culture.

Plan the timing of the presentation of engagement results to avoid undue delay.

Disseminating Results

The Director of Internal Audit will communicate results to the appropriate parties.

The Director of Internal Audit or designee reviews and approves the final engagement communication before issuance and decides to whom and how it will be disseminated.

The internal auditors will discuss conclusions and recommendations with appropriate levels of management before the Director of Internal Audit issues the final engagement communications. This is usually accomplished during the course of the engagement and/or at post-engagement meetings (i.e., exit meetings).

Another technique is for the management of the audited activity to review draft engagement issues, observations, and recommendations. These discussions and reviews help avoid misunderstandings or misinterpretations of fact by providing the opportunity for the engagement client to clarify specific items and express views about the observations, conclusions, and recommendations.

The level of participants in the discussions and reviews vary by nature of the report; they generally include those individuals who are knowledgeable of detailed operations and those who can authorize the implementation of corrective action.

The Director of Internal Audit distributes the final engagement communication to the management of the audited activity and to those members of the University who can ensure engagement results are given due consideration and take corrective action or ensure that corrective action is taken.

Where appropriate, the Director of Internal Audit may send a summary communication to higher-level members in the University. Where required by the Internal Audit Charter or University policy, the Director of Internal Audit also communicates to other interested or affected parties such as external auditors and the Audit Committee.

Monitoring Progress

The Director of Internal Audit will establish and maintain a system to monitor the disposition of results communicated to management.

To effectively monitor the disposition of results, the Director of Internal Audit will establish procedures to include:

- The timeframe within which management's response to the engagement observations and recommendations is required.
- Evaluation of management's response.
- Verification of the response (if appropriate).
- Performance of a follow-up engagement (if appropriate).
- A communications process that escalates unsatisfactory responses/actions, including the assumption of risk, to the appropriate levels of senior management or the Audit Committee.

If certain reported observations and recommendations are significant enough to require immediate action by management or the Audit Committee, the Internal Audit

Department monitors actions taken until the observation is corrected or the recommendation implemented.

The Internal Audit Department will effectively monitor progress by:

- Addressing engagement observations and recommendations to appropriate levels of management responsible for taking action.
- Receiving and evaluating management responses and proposed action plan to engagement observations and recommendations during the engagement or within a reasonable time period after the engagement results are communicated. Responses are more useful if they include sufficient information for the Director of Internal Audit to evaluate the adequacy and timeliness of proposed actions.
- Receiving periodic updates from management to evaluate the status of its efforts to correct observations and/or implement recommendations.
- Receiving and evaluating information from other organizational units' assigned responsibility for follow-up or corrective actions.
- Reporting to senior management and/or the Audit Committee on the status of responses to engagement observations and recommendations.

Follow-up Process

The Director of Internal Audit must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

The internal auditors determine whether management has taken action or implemented the recommendation. The internal auditor determines whether the desired results were achieved or if senior management or the Audit Committee has assumed the risk of not taking action or implementing the recommendation.

Follow-up is a process by which internal auditors evaluate the adequacy, effectiveness, and timeliness of actions taken by management on reported observations and recommendations, including those made by external auditors and others. This process also includes determining whether senior management and/or the Audit Committee have assumed the risk of not taking corrective action on reported observations.

The Internal Audit Department's Charter defines the responsibility for follow-up. The Director of Internal Audit determines the nature, timing, and extent of follow-up, considering the following factors:

- Significance of the reported observation or recommendation.
- Degree of effort and cost needed to correct the reported condition.
- Impact that may result should the corrective action fail.
- Complexity of the corrective action.
- Time period involved.

The Director of Internal Audit is responsible for scheduling follow-up activities as part of developing engagement work schedules. Scheduling of follow-up is based on the risk and exposure involved, as well as the degree of difficulty and the significance of timing in implementing corrective action.

Where the Director of Internal Audit judges that management's oral or written response indicates that action taken is sufficient when weighed against the relative importance of the observation or recommendation, internal auditors may follow up as part of the next engagement.

Internal auditors ascertain whether actions taken on observations and recommendations remedy the underlying conditions. Follow-up activities should be appropriately documented.