Purpose

The purpose of the auditor's RA is to provide assurance that internal controls in place are adequate to mitigate risks and achieve the organization's goals. The Internal Audit (IA) Department uses the RA to develop effective allocation of audit resources to examine auditable units in the audit universe and select areas for review that have the greatest risk exposure. While management has responsibility to develop and maintain a system to identify and mitigate risk, IA's goal is to assist the University by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems. Our efforts will be focused on establishing risk-based plans to determine the priorities of the internal audit activity and assess management's risk mitigation activities, all to develop the annual audit plan, with your input and final approval by the Board of Visitors. Per the Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing (Standards)*, the internal audit activity's plan of engagements should be based upon a Risk Assessment (Standard 2010.A1).

The IIA *Standards* define risk as "the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood." In addition, the IIA *Standards* define risk management as "A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives." Ultimately, key audit objectives are to provide management with information to mitigate the negative consequences associated with accomplishing the University's objectives, as well as an assessment of the effectiveness of management's risk management activities.

1. <u>Business Processes</u>

   Using Microsoft Word, please provide a current list of the Business Processes (functions) and corresponding responsibilities performed within the Assessable Units (Departments) under your control and direction. A business process is defined as a collection of related, structured activities--a chain of events--that produce a specific service or product for a particular customer or customers. An assessable unit is an ongoing, identified purpose that results in the creation of a service or product (used either internally or externally) or that fulfills a law, regulation or other mandate. Accepted best practices indicate that management should maintain a listing of the assessable units along with the purpose and objectives of each assessable unit. Please note, an Assessable Unit can have many Business Processes (functions); this is not a one-to-one relationship, but possibly a one-to-many relationships.

2. <u>Risk Analysis Surveys</u>

   Please complete the enclosed questionnaire for each of the Business Processes with the Assessable Units under your responsibility. Your honest and objective assessment will contribute to the University strategic plan to mitigate University-wide risks.

Some items you may wish to consider as you complete the Risk Analysis are:

- Control self assessments
- Staff turnover and experience level
- Staff training assessment and development

Risk Analysis Surveys – Operational

- New technology implementations
- Degree of complexity in operational and/or technical processes
- Exposure to external reviews and reputational risk
- Degree of compliance and regulatory requirements
- Results of internal and external audits and audit frequency
- Vulnerability of errors, omissions, losses or fraud

Please read each of the questions carefully. Mark the applicable Business Risk level for each of the questions. You must choose a degree of risk using the numbers 1 through 3, where 1 indicates the lowest risk and 3 indicates the highest risk. If the risk level of a question is scored as a 1 or a 3, provide a brief justification for the score in the Assessable Unit Comments section following that question. However, please feel free to comment on any rating selected.

Attached you will find a list of definitions (Appendix A) that might help you as you complete the Risk Analysis Survey. Please call any member of the Internal Audit team at ext. 5295n or 5371 if you have any questions. Your cooperation is greatly appreciated.

Appendix A – Definitions

Assessable Unit: An assessable unit is an ongoing, identified purpose that results in the creation of a service or product (used either internally or externally) or that fulfills a law, regulation or other mandate.

Business Process: A collection of related, structured activities--a chain of events--that produce a specific service or product for a particular customer or customers; significant activities that are carried out to achieve the University's mission and objectives, i.e. 20/20 Vision Plan. A business process can be thought of as a "cookbook" for running the University and reaching University goals defined in an organization's business strategy. Business processes occur at all levels of an organization's activities and include events that the customer sees and events that are invisible to the customer.

Controls: Any action taken by management, the board, and other parties to manage risk to 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. Basic controls usually ensure the reliability and integrity of information; ensure compliance with policies, laws, regulations, etc.; safeguard assets; promote economical and efficient use of resources; and accomplish goals and objectives.

Control Activities: These are the policies and procedures that help ensure management that management directives are implemented. Control activities consist of non-financial and financial activities, occur at all levels of the organization, such as performance reviews, functional or activity reviews, transaction reviews, academic record keeping, reconciliations, processing controls, physical controls and segregation of duties. Some typical controls seen every day are:

1. Transaction Authorizations - to ensure that all transactions are approved by responsible personnel in accordance with their specific or general authority before the transaction is recorded.
2. Documentation - all back-up documentation required is properly maintained.
3. Review For Completeness - to ensure that no valid transactions have been omitted from the accounting records.
4. Accuracy - to ensure that all valid transactions and/or reports are accurate, consistent with the originating transaction data, and information is recorded in a timely manner.
5. Validity (fairly represents events) - to ensure that all recorded transactions fairly represent the economic events that actually occurred, are lawful in nature, and have been executed in accordance with management's general authorization.
6. Physical Safeguards - to ensure that access to physical assets and information systems is controlled and properly restricted to authorized personnel.
7. Error Handling - to ensure that errors detected at any stage of processing receive prompt corrective action and are reported to the appropriate level of management.
8. Segregation Of Duties - to ensure that duties are assigned to individuals in a manner that ensures that no one individual can control both the authorization and recording functions or the procedures relative to processing or approving a transaction.

A well designed process with appropriate internal controls should meet most if not all of these control objectives.

Control Deficiency: When the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

Risk Analysis Surveys – Operational

Control Environment: This sets the tone of the organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the organization's people; management's philosophy and operating style; the way management assigns authority and responsibility; how it organizes and develops its human resources; and the attention and direction provided by the Board of Visitors.

Control Self-Assessment (CSA): An internal control evaluation tool that involves management and staff in the "self-assessment" of internal controls within their work group. It is a documented process in which management or work teams directly involved in the function or process to be assessed, are given the ability to evaluate the effectiveness of the process in place and decide if the chance of reaching some or all business objectives is reasonably assured. A CSA usually consists of questions that are used as a general guide to help managers ensure that basic internal controls are in place. A "yes" answer indicates that a desired control is in place; a "no" answer indicates that a control weakness may be present, and corrective action may be necessary.

Monitoring: This is the process that assesses the quality of the system's performance over time. Ongoing monitoring is the daily review of reports, supervision and self-assessment. Separate evaluations external to the unit are carried out on a periodic basis.

Risk Assessment: Risk assessment is the identification and analysis of the risks relevant to the achievement of the organization's objectives. Assessment may include looking at departmental routines, activities, and personnel, identifying any potential problems. This forms the basis for determining how the risks should be managed.