1. In your opinion, what is the primary risk, if any, facing your unit? What mitigating controls, if any, are in place?

2. Are you aware of any area in your unit that may have weak internal controls? If so, is the potential for fraud to occur strong, moderate, or low?

3. For the issues you are responsible for, do you believe there is a strong overall control environment to protect the University’s resources? If there is not, please explain in which area you believe there may be weaknesses.

4. Do you believe that the University has effective preventive controls, such as segregation of duties, information security, authorization requirements, and physical safeguards, to prevent undesirable events from occurring? If not, please explain why you feel this way.

5. In your opinion, which functional area(s) in the University do you believe possess high financial risk—where, if the controls do not work, there could be a loss of monetary resources or physical assets?

6. Are the University’s policies and procedures clear, comprehensive, and effectively communicated? Are they used to guide the actions of your unit?

7. Does the University’s financial reporting system (including software, reports, and personnel) provide you with relevant, accurate, and timely information to assist you in achieving your objectives? If the answer is no, what specifically do you think is needed?

8. For other than high risk areas, how often should each unit in the University be audited? In other words, should our audit cycle be every 2 years? 3 years? 5 years?
DEFINITIONS

Risk - any activity that prevents an organization from achieving its objectives. Five types of risk:
- Strategic - prevents University from achieving its goals
- Financial - may result in loss of assets (monetary or physical assets)
- Operational - adversely affects an ongoing management process
- Compliance - violates a law, regulation, or internal policy
- Reputation - harmful to the University’s reputation (an external perception)

Internal controls - process designed to provide reasonable assurance regarding achievement of objectives in the following categories:
- effectiveness and efficiency of operations
- reliability of financial reporting
- compliance with applicable laws and regulations
The central theme of internal control is to identify risks and to do what is necessary to manage those risks.

Mitigating controls/control activities - actions, supported by policies and procedures that, when carried out properly and in a timely manner, manage or reduce risk.

- Preventive control - a proactive attempt to deter or prevent undesirable events from occurring (examples: segregation of duties, proper authorization, adequate documentation, and physical control over assets)

- Detective control - an attempt to detect undesirable acts; provide evidence that loss has occurred but do not prevent a loss from occurring (examples: reconciliations, reviews, variance analyses, physical inventories, and audits)

Fraud - There are generally three requirements for fraud to occur: motivation, opportunity, and personal characteristics. Opportunity is the easiest and most effective requirement to address to reduce the probability of fraud. By developing effective systems of internal control, you can remove opportunities to commit fraud.

Control environment - the tone at the top; control-consciousness throughout the organization’s culture. It is the atmosphere in which people conduct their activities. An effective control environment is where competent people understand their responsibilities, the limits to their authority, and are knowledgeable, mindful, and committed to doing what is right and to doing it the right way. In other words, it encompasses technical competence and ethical commitment.