Internal Controls at the University of Pennsylvania
Internal Control - Defined

- A process, effected by the board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
  - Reliability of financial reporting
  - Effectiveness and efficiency of operations
  - Compliance with applicable laws and regulations
What Do Internal Controls Do?

- Internal Controls are designed to:
  - Safeguard Assets
  - Ensure that all transactions are recorded and that all recorded transactions are legitimate
  - Protect the University & its employees from accusations of wrongdoing & litigation
  - Ensure the effective and efficient use of University resources
In a Nutshell

- Internal Controls help to ensure that you will be able to successfully achieve the goals and objectives of your department.
Who Is Responsible For Internal Controls?

Everyone plays a part in Penn’s internal control system. Ultimately, it is management's responsibility to ensure that controls are in place. This responsibility is delegated to the leadership of each area of operation. Every employee has some responsibility for making this internal control system function. Therefore, all Penn employees need to be aware of the concept and purpose of internal controls.
Internal Control Policies

• Section 2700 of the Financial Policy Manual

• Highlights:
  – 2701 Internal Control Policy
    • Comptroller has ultimate responsibility for the adequacy and effectiveness of the overall system of internal control.
    • Because of decentralization, schools, service and resource centers, central administrative departments, auxiliary enterprises, ... are required to develop, implement, and monitor a system of internal controls
    • Requires documentation of internal control systems (e.g. written policies & procedures, org charts, job descriptions, flow charts and process narratives)
  – 2702 Internal Audit
    • OACP has the authority to recommend improvements and to monitor the implementation of its recommendations. It has free, unlimited and unrestricted access to all books, records, files, property and personnel of the University and the Health System.
Components of Control

- Control Environment
- Risk Assessment
- Control Activities
- Monitoring
Control Environment

• Foundation for your system of internal control
• “Tone at the Top”
• Includes:
  – Integrity & Ethical Values
  – Commitment to Competence
  – Leadership’s Philosophy & Operating Style
  – Organizational Structure and Personnel Development
Risk Assessment

• Ask yourself
  – What could go wrong?
  – What assets should we be protecting?
  – What do we do to prevent theft/fraud?
  – What activities are regulated by the federal government (or other regulatory body)?
  – What external exposures might we have?
  – How would this look to an outsider?
Control Activities

- Monitoring
- Control Activities
- Risk Assessment
- Control Environment
Control Activities

• Actions or procedures that manage or reduce risk

• Preventive and Detective Controls
  – Preventive – stops undesirable events/outcomes
  – Detective – detects undesirable events after the fact
Examples of Control Activities

• Policies & Procedures
• Authorization & Approvals
• Verification, Reconciliation, and Review
• Physical security of assets (safes, lockboxes, locked doors, etc)
• Segregation of duties
• Adequate Documentation
Information & Communication

- Monitoring
- Control Activities
- Risk Assessment
- Control Environment
Information & Communication

• Pertinent information must be identified, captured and communicated to appropriate personnel on a timely basis.

• Effective communication also must occur in a broader sense, flowing down, across and up the organization.
Monitoring

Control Activities

Risk Assessment

Control Environment

Information & Communication
Monitoring

• The process that assesses the quality of the internal control system’s performance over time.

• Necessary because the way controls are applied may evolve or changes to circumstances for which the internal control system was originally designed.

• Accomplished through:
  – Ongoing monitoring in the course of operations
    • Includes regular management and supervisory activities
  – Separate evaluations
    • Focused examination by management or Internal Audit
Limitations of Internal Control

- Judgment – decisions are made in the time available, based on information at hand, and under pressures to conduct business
- Breakdowns – personnel may misunderstand instructions or procedure, mistakes, errors due to new technology or complexity of information systems
- Management Override – overrule prescribed policies or procedures for personal gain or advantage
- Collusion – individuals acting collectively can commit fraud and alter records so as to avoid detection by the internal control system
Control Tips

• Create a Strong Control Environment:
  – Set the proper tone for your work environment under which “doing right” is not only encouraged, but clearly expected;
  – Create an environment in which it is okay to ask questions;
  – Don’t assume that superiors or subordinates understand the risks, discuss them freely;
  – Apply the *Inquirer test*
  – Do not compromise your standards and ethics or expect others to
  – Accept responsibility and accountability and expect the same in those who work with you
Control Tips – Segregation of Duties

- No single individual should have control over 2 or more phases of a transaction or operation.
- Phases are:

<table>
<thead>
<tr>
<th>Authorization</th>
<th>Custody</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record Keeping</td>
<td>Reconciliation</td>
</tr>
</tbody>
</table>

- Makes deliberate fraud more difficult because it requires collusion of 2 or more persons
- Makes it much more likely that innocent errors will be found
- When responsibilities can’t be completely segregated, compensating controls must be implemented
Control Tips – Cash Receipts

• Segregate duties
• Provide receipts (pre-numbered/retain copies)
• Deposit daily
• For deposit only/Account # stamp
• Secure funds while they’re in your possession
Control Tips – Petty Cash

- Restrict access to the custodian only.
- Secure the cash box
- No check cashing, advances, loans, etc.
- Use petty cash vouchers (w/ names/signatures)
- Require receipts & review for compliance w/ policies
- Custodian’s supervisor (who TAC’s the replenishment should reconcile the fund to ensure accuracy & to deter/detect fraud)
- Management performs surprise counts
Control Tips – Purchasing Card

- Supervisors must review the transactions to ensure legitimacy of business purpose, compliance w/ University policies
- Secure the card (and use it for University business only)
- Maintain all receipts
- Print the monthly statement from PaymentNet & attach receipts
- Sign & date the monthly statement & submit for supervisory review
Control Tips – Travel

- Detailed receipts
- Ensure only allowable items
- Submitted within 60 days of travel
- Sufficient business purpose
- List of attendees & their affiliation
- Support for foreign currency conversion
- Alcohol charged to 5214
- Properly authorized?
Control Tips – HR/Payroll

- Verify accuracy of employee record/pay rates for new employees
- Time sheets/cards approved by supervisor
- Prior approval of extra pay & overtime
- Regular monitoring/reconciliation of payroll
- Utilization of a termination checklist
- Performance of regular performance evaluations
Control Tips – Gifts & Endowments

• Ensure the gift agreement is available for reference by fund administrators over the life of the gift to ensure proper utilization in agreement with the donor restrictions

• Monitor the funds regularly to identify surpluses. Donors expect monies to be utilized, not hoarded.

• In instances when funds can’t be utilized, identify opportunities to reinvest the funds to demonstrate effective stewardship of donated funding.
Control Tips – Grants Administration

- Expenditures are reviewed for allowability, classification, and adequate funding prior to payment
- Documentation
- Sub-award monitoring
- PI approval of expenditures
- PBUD/PBIL/Budget
- A/R Monitoring
- Deficit Monitoring
- Cost transfers
Control Tips – Information Systems

• Never share passwords with anyone (Not your co-worker, your backup, your supervisor, the system administrator...)

• Secure passwords (No Post-it note on the monitor. Or in the top desk drawer)

• Make passwords complex (hard to guess)
  – Don’t use names or dictionary words
  – Don’t use alphanumeric series (abcdefg, 1234567)
  – Combine letters & numbers, upper & lower case, use characters when possible