The Basics of Internal Controls

Presented to:

The Institute of Internal Auditors (IIA)
Topeka Chapter

April 7, 2009
Today’s Objectives

Provide Insight into Internal Controls!

- Risk and Fraud – the basis for controls
- Internal controls defined
- 5+1 internal control components
- Steps for ensuring control
What Is Risk?

Anything that could negatively impact the organization’s ability to meet it’s operational objectives.

- The purpose behind controls
5 Types of Risk

- **Strategic** – risk that would prevent an organization from accomplishing its objectives (meeting its goals).
- **Financial** – risk that could result in a negative financial impact to the organization (waste or loss of assets).
- **Regulatory (Compliance)** – risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations.
- **Reputational** – risk that could expose the organization to negative publicity.
- **Operational** – risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations.
How To Identify Risk

**For each department/division objective, ask:**

- What could go wrong? How could we fail?
- What must go right to succeed?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- On what do we spend the most money?
- How do you bill/collect related revenue?
- On what information do we most rely?
- What assets do we need to protect?
- How could someone or something disrupt our operations?
Conditions That Increase Risk

- Lack of segregation of duties
- Too much trust
  - Approval of documents without review
  - Lack of verification of transactions after they have been entered in the system
  - Lack of reconciliations
- No follow-up when things appear “questionable” or “not reasonable”
- Lack of control over cash/petty cash
- Lack of control over purchasing of materials/supplies
- Lack of knowledge of policies and procedures
What Is Fraud?

Legal Definition of Fraud

“All multifarious means which human ingenuity can devise, and which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth. It includes all surprises, tricks, cunning or dissembling, and any unfair way which another is cheated.”

What Is Fraud?

Fraud is a common risk that should not be ignored. The incidence of fraud is now so common that its occurrence is no longer remarkable, only its scale.

Any entity that fails to protect itself appropriately from fraud should expect to become a victim of fraud, or rather, should expect to discover that it is a victim of fraud.

There is no such thing as an accidental fraud. What separates error from fraud is *intent*; the accidental from the intentional.
Causes of Fraud

Poor internal control creates *opportunity* for fraud.
Fraudulent Behavior Examples

- Payment to fictitious vendor
- Diversion of cash receipts
- Extra compensation to perpetrator
- Personal benefit from travel expenses
- Restricted funds manipulation
- Use of IT systems for personal/illegal activity
- Mis-statement of corporate results
How Does Fraud Occur?

- Poor internal controls
  - Lack of proper authorization
  - No separation of authorization, custody, record keeping
  - No independent checks on performance
  - Lack of clear lines of authority
  - Inadequate documentation
- Management override of internal controls
- Collusion between employees and 3rd parties
- Collusion between employees and management
- Poor or non-existent ethics policy
- Limited, unclear or no policies and procedures to direct business function processes
How To Mitigate Risk & Fraud

Implement Internal Control Framework
What Are Internal Controls?

- Keeping an eye on organization assets and resources.
- Finding ways to make sure people don’t do bad things.
- Protecting the organization from being accused of doing bad things.
- Good, sound business practice.
- Common sense!
Definition of Internal Control

Internal control is a process designed to provide reasonable assurance regarding the achievement of objectives in the following areas:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Safeguarding assets
Examples of Internal Control

Think about what *you* do.....

- Lock your home and vehicle.
- Keep your ATM/debit card pin number separate from your card.
- Review bills and credit card statements before paying them.
- Reconcile your bank statement.
- Don’t leave blank checks or cash just lying around.
- Expect your children to ask permission before they can do certain things.
- Other examples.....??
Department Internal Controls

- Computer passwords are periodically changed and shouldn’t be written down or kept by the PC.
- Check purchase card charges against source documents.
- Check management reports against source documents.
- Lock cash drawers and secure storage for checks.
- Authorizations required for certain activities.
- Other examples....??
Internal Control Components

▪ **Control Environment**

The foundation on which everything rests.

Key factors:
- Management’s attitude: “Tone at the Top”
- Individual attributes: integrity, ethical values, competence

Examples:
- Strategy
- Policy
- Training
Internal Control Components

- **Risk Assessment**

  Management must be aware of, anticipate and deal with risks.

  Management must establish methods and mechanisms to identify, analyze and manage risks that are likely to have an impact on service delivery and the achievement of desired outcomes.
Internal Control Components

- **Risk Assessment**

  Change is an indicator of risk
  - new personnel
  - new information system and/or technology
  - rapid growth
  - new programs/services

  Inherent risk
  - complexity
  - cash receipts
Internal Control Components

- **Control Activities**

  Control activities are the actions supported by policies and procedures that help assure management directives to address risks are carried out properly and timely.
Internal Control Components

- **Control Activities**

To be effective, control activities must be:
- Appropriate;
- Functioning consistently according to plan throughout the period;
- Cost effective, comprehensive, reasonable;
- Directly related to the control objective; and
- Derive from a defined risk to the organization.
5 Internal Controls (+1)

- **Types of Control Activities**
  - Directive
  - Preventive
  - Detective
  - Corrective
  - Recovery
  - (Automated)
Internal Control Components

- **Control Activities**

  **Examples of Directive Controls:**
  - Setting corporate policies, department policy/procedures;
  - Setting spending limits
  - Setting IT configuration standards;
  - Other examples??
Internal Control Components

- **Control Activities**

**Examples of Preventive Controls:**
- ✔ Training on applicable policies, department policy/procedures;
- ✔ Review and approval process for purchase requisitions to make sure they are appropriate before the purchase;
- ✔ IT access authorizations to ensure access is appropriate;
- ✔ The use of passwords to stop unauthorized access to systems/applications;
- ✔ Other examples??
Internal Control Components

- **Control Activities**

**Examples of Detective Controls:**
- Cash counts; bank reconciliation;
- Review your payroll reports;
- Compare transactions on reports to source documents;
- Monitor actual expenditures against budget;
- Review logs for evidence of mischief;
- Other examples??
Internal Control Components

- **Preventive vs. Detective**

**Preventive**
- ✓ Authorization and approval procedures;
- ✓ Supervision (assigning, reviewing/approving, guidance, training);
- ✓ Segregation of duties (authorizing, processing, recording, reviewing);
- ✓ Controls over access to resources and records;

**Detective**
- ✓ Reviews of operating performances;
- ✓ Reconciliations;
- ✓ Verifications;
- ✓ Reviews of processes and activities.
Internal Control Components

- **Control Activities**

**Examples of Corrective Controls:**
- Submit corrective journal entries after discovering an error;
- Complete changes to IT access lists if individual’s role changes;
- Other examples??
Internal Control Components

- **Control Activities**

**Examples of Recovery Controls:**
- Prepare data backups from current systems
- Storing documents and IT backups in a protected environment to ensure availability
- Restore data from backup following a failure;
- Other examples??
Internal Control Components

- **Control Activities**

  **Examples of Automated (IT) Controls:**
  - IT access permissions;
  - System password requirements;
  - Preset spending limits;
  - Other examples??
Internal Control Examples

**Invoice Processing**

- Formal policy/procedure on processing (*Directive*)
- Must be matched to Materials Received (*Preventive*)
- An additional signature is required (*Preventive/Manual*)
- Online entry and authorization are separated (*Preventive/Automated*)
- Preset authorization levels (*Preventive/Automated*)
- Report of processed invoices reviewed and matched against paper invoices/materials received (*Detective*)
- Invoice matching reports reviewed by Internal Audit for proper review (*Detective*)
- Incorrect invoices adjusted and resubmitted (*Corrective*)

Private and Confidential
Control Examples (IT)

**IT Application Access**
- Formal policy/procedure on access (*Directive*)
- Access control Roles established in application/system (*Preventive/Automated*)
- Access requested by individual or supervisor (*Preventive/Manual*)
- Access request approval by management (*Preventive/Manual*)
- Access validation process in application/system (*Preventive/Automated*)
- Report of access reviewed by management periodically (*Detective*)
- Inappropriate access removed (*Corrective*)
- Access permissions reloaded to system when inadvertently altered/lost (*Recovery*)
Case Study – Missing Camera

Joe, the hard working staff assistant, is asked to process a requisition to purchase a new $5,000 camera to be used by a project manager who is working on a federal grant project. Later, when Joe conducts the annual physical inventory for the department, as requested by the Accounting Department, he is not able to locate the camera in the department. Joe learns the project manager was given permission by the department manager to take the camera home so that he could take photos at his sister’s wedding (that was 2 months ago). When Joe talks to the department director about it, he is told not to worry – since the camera wasn’t purchased with company funds (i.e., the grant paid for it), it would be okay to check it off on the inventory report even though it had been removed from the premises.
Case Study – The New TV

Jill, a senior staff assistant, is the department’s procurement card holder. Her department manager, Anna, travels extensively so Jill occasionally uses a signature stamp to approve her procurement card statements. Jill went shopping for a new TV one weekend. While checking out, Jill mistakenly used her company procurement card. On Monday she received an email from Payme.net confirming the purchase; at that time she realized her mistake.

Jill decided to wait until Anna returned from out of town to ask her advice. Jill was certain Anna would understand and help her straighten things out. The statement arrived a week later and Jill had Jack, the office assistant, approve the statement since Anna wasn’t due back for another two weeks.

Upon Anna’s return, Jill had not saved enough money to repay the company for the TV. Since Anna had not seen the statement and it had already been processed by Accounting, Jill decided not to bring it up. She had been an exceptional employee for years and had seen many of her coworkers receive bonuses. She decided it was her turn. This would be her bonus. She had earned it!
Internal Control Pyramid

Is it Working?
- Approvals
- Reconciliation
- Physical and technical safeguarding of assets
- Segregation of duties

Controls

Risks

Identify the things that “keep me up at night”

Policies and Procedures; overall tone from Management

Experience. Results. Value.
Why Controls Don’t Always Work

- Inadequate knowledge of policies or governing regulations.
  - “I didn’t know that!”
- Inadequate segregation of duties.
  - “We trust ‘A’ who does all of those things.”
- Inappropriate access to assets.
  - Passwords shared, access not removed, cash not secured...
- Form over substance.
  - “You mean I’m supposed to do something besides initial/sign it?”
Why Controls Don’t Always Work

- Control override.
  - “I know that’s the policy, but we do it this way.”
  - “Just get it done; I don’t care how!”

- Inherent limitations.
  - People are people and mistakes happen. You cannot foresee or eliminate all risk.
Ensuring Control

When thinking about internal controls, consider the following:

- **Propriety of transactions**...is this legal and right? Does it feel or look wrong? Would someone else think so?
- **Reliability and integrity of information**...is the information/form/data/report accurate and complete?
- **Compliance with policies and government regulations**...are you following established procedures/instructions?
- **Safeguarding assets**...could anyone take or gain access to items under your control without being observed?
- **Economy and efficiency of operations**...is there a better way to do the job?

Does it address a risk of significance to the organization?
Ensuring Control

- Make sure you have up-to-date policies and procedures;
- Ensure authorization limits are communicated within your department;
- Ensure all assets (especially cash) are safeguarded at all times;
- Establish document control (especially for spreadsheets);
- Ensure approval signatures are visible (legible) on all required documentation;
- Make sure data is only accessible by authorized personnel;
- Understand your department/function’s risks;
- Ensure adherence to policy and legal/regulatory requirements;
- Establish objectives and measures for your department/function and for major programs; and
- Track performance to evaluate your success!
Questions?
Today’s Presenter

- Richard Mosher, CISSP, CBCP, CISA, CGEIT, QSA
  - 23 years in information security
  - 10 years in Business Continuity Management/Disaster Recovery
  - 6 years in IT auditing
  - Specialist in policy, procedures, standards, governance and compliance
- Phone: 816-627-4216
- E-mail: Richard.Mosher@jeffersonwells.com

Jefferson Wells is a global provider of professional services in the areas of risk, controls, compliance and financial process improvement. The firm specializes in internal audit, technology risk management, tax, and accounting and finance.