Introduction – What Is Risk Assessment and Risk Management?

"Internal Controls and You" (risk assessment and risk management training)

Presented by:
The University of Toledo Internal Audit Department
David L. Cutri, Chief Audit Executive
530-8718

COURSE AGENDA

DAY ONE

Unit Number	Description
Unit 1	Introduction – What Is Risk Assessment and Risk Management?
Unit 2	What Is Internal Control? The COSO Report
Unit 3	Identifying Controls
Unit 4	Internal Control Game
Unit 5	Designing and Evaluating Controls
Unit 6	Special Cases and Challenges

DAY TWO

Group Activity
Wrap-up and Evaluations

Introduction – What Is Risk Assessment and Risk Management?

Overview

This course covers the essential terminology of risk and control. It also provides an overview of commonly used risk and control frameworks. In addition, examples of how to critically evaluate risks for your organization are provided.

UNIT ONE

INTRODUCTION – WHAT IS RISK ASSESSMENT AND RISK MANAGEMENT?

Overview

This unit covers introductions and provides an overview of this seminar.

Objectives

In this unit, you will

- Meet the instructor and your fellow participants
- Learn what to expect during the next 1 ½ days

Introduction – What Is Risk Assessment and Risk Management?

Participant Introductions

Name_____ Department_____

Department Size: _____ Time in Department: _____

Your background before your current role (or instead of current role) _____
_____
_____

Types of internal control activities you perform (financial, operational, compliance, IT, fraud, etc.), or the function you perform in your organization (if you do not (or do not know if you) perform internal control activities):
_____
_____

Your expectation or goal(s) for this course_____
_____
_____

Something interesting (or fun) about yourself_____
_____
_____

Introduction – What Is Risk Assessment and Risk Management?

Pre-Test

Circle all that apply:

1. Internal control is:
    a. policies and procedures
    b. how people feel about their work
    c. serving customers
    d. a dirty word

2. Lack of internal control can lead to:
    a. loss of assets
    b. poor management decisions
    c. poorly written reports by examiners and regulators
    d. excessive CEO compensation
    e. loss of customers

3. Review by someone independent of an activity is a control if it is done to:
    a. detect errors
    b. identify ways to improve the process
    c. detect fraud

Introduction – What Is Risk Assessment and Risk Management?

Pre-Test

(Continued)

4. Which of the following are internal controls?
   a. authorizations
   b. team meetings
   c. statistical process control
   d. open communications
   e. reconciliations
   f. issuing a press release
   g. strategic planning
   h. purchasing supplies
   i. reviews of operating performance
   j. vendor partnerships

5. Which of the following contribute to effective control:
   a. an atmosphere of trust
   b. requiring adherence to defined policies, regardless of the circumstances
   c. a “suggestion box” program

Perspectives on Internal Control

"What's in it for me that would cause me to shift some of my time, which is quite precious to me, into a concentrated effort that results in good internal control?

> … You call it invoicing and payables and issues, and a lot of other things: I call it profit… Business is a dynamic process. New and different deals are being made every day. Control is simply the process that keeps the money coming in and going out in the proper amounts in line with the ever changing ways we do business.
>
> … You think physical inventory, reconciliations and periodically checking the equipment in the mill to the list of fixed assets; I think confidence -- confidence that we're addressing real problems in our decision-making process. For example, any decision I make about your mill is based upon what you report about your mill. Like it or not, I know more about your business after a few minutes of reading your reports than I do after a day of touring the facility. More, that is, if the reports are accurate."
>
> - from a speech on internal controls by a Business Vice President of Weyerhaeuser Company

"Internal control gets us where we want to go, without surprises along the way. Internal control is everyone's responsibility… Internal control is me."

- from Cargill Corporation's Internal Control Statement

"Control… support(s) people in the achievement of the organization's objectives… Control is what makes an organization reliable in achieving its objectives."

- from *Guidance on Control*, The Canadian Institute of Chartered Accountants

Introduction – What Is Risk Assessment and Risk Management?

Objectives

By the end of this course, you should be able to:

- Identify the components of risk assessment and risk management as they relate to internal controls.
- Establish a risk management and internal controls strategy for your business unit
- Identify and be able to apply key University policies and procedures.

THE UNIVERSITY OF TOLEDO 1872

Program Objectives

By the end of this seminar, you should be able to:

- Understand what internal control is and is not
- Design control systems for business processes
- Analyze and evaluate existing or planned control systems

Introduction – What Is Risk Assessment and Risk Management?

Program Topics

- Internal Control Myths and Reality
- What Is Internal Control? The COSO Report
- Internal Control Game
- Identifying Controls
- Designing Controls
- Evaluating Controls
- Special Cases and Challenges

Internal Control Myths

Myths

- Internal control starts with a strong set of policies and procedures
- "Internal control – that's what I have internal auditors for!"
- "Internal control is a finance thing. We do what the Controller's office tells us to do."
- Internal control are essentially negative, like a list of "thou shall not's"
- Internal controls are a necessary evil. They take time away from our core activities – making product, selling, and serving customers
- With downsizing and empowerment, we have to give up a certain amount of control
- If controls are strong enough, we can be sure there will be no fraud, and financial statements will be accurate

Internal Control Myths and Realities

Myths	Realities
• Internal control starts with a strong set of policies and procedures	✓ Internal control starts with a strong control environment
• "Internal control – that's what I have internal auditors for!"	✓ Management is the owner of internal control
• "Internal control is a finance thing. We do what the Controller's office tells us to do."	✓ Internal control is integral to every aspect of the business
• Internal control is essentially negative, like a list of "thou shall not's"	✓ Internal control makes the right things happen the first time – and every time.
• Internal controls are a necessary evil. They take time away from our core activities – making product, selling, and serving customers	✓ Internal controls should be "built into, not onto" business processes
• With downsizing and empowerment, we have to give up a certain amount of control	✓ With downsizing and empowerment, we need different forms of control
• If controls are strong enough, we can be sure there will be no fraud, and financial statements will be accurate	✓ Internal control provides reasonable, but not absolute assurance that the organization's objectives will be achieved

Introduction – What Is Risk Assessment and Risk Management?

What Is Business Risk Management?

- "A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives" (The Institute of Internal Auditors)

- In other words, business risk management is the identification of key **business objectives** within a process, **risks** to achieving these business objectives, and the internal **controls** in place to resolve the risks identified.

THE UNIVERSITY OF TOLEDO 1872

Practice Advisory 2100-1: Nature of Work

The scope of risk management and risk assessment should encompass a systematic, disciplined approach to evaluating and improving the **adequacy** and **effectiveness** of risk management, control, and governance processes and the quality of performance in carrying out assigned responsibilities.

The **purpose** of evaluating the adequacy of the organization's existing risk management, control, and governance processes is to provide reasonable assurance that these **processes are functioning as intended** and will enable the organization's objectives and goals to be met, and to **provide recommendations for improving** the organization's operations, in terms of both efficient and effective performance.

Identifying Risks

Definition of Risk: Anything that could jeopardize the achievement of an objective

To identify risks

For each objective, ask common sense questions like the following:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What resources do we need to protect (physical, information, human)?
- Do we have liquid assets or assets which could be used by others easily?
- How could someone steal from us?
- How could someone disrupt our operations?
- How do we know whether we are achieving our objectives?
- On what information do we rely most?
- On what do we spend the most money?
- What decisions require the most judgment?
- What activities are most complex?
- What activities are regulated?
- What is our greatest legal exposure?

Some of these questions may lead to risks which do not relate to the objective you start from – or any of the other objectives you've defined. If the risk is significant, this probably means you have another objective to define.

Introduction – What Is Risk Assessment and Risk Management?

Who Is Responsible for Business Risk Management?

YOU !!!

(the process owner)

Roles and Responsibilities

Management is directly responsible for internal controls. In particular, the

- **CEO/President** is the "owner" of the internal control system.
- **Other managers** are effectively the chief executives of their sphere of responsibility.

Other personnel all play a role in the process of internal control.

Board of Directors/Board of Trustees provides guidance and oversight.

The **internal audit** function does not have primary responsibility for establishing and maintaining internal controls. Internal auditors play an important role in evaluating the effectiveness of control systems and, thereby, contribute to ongoing effectiveness.

External parties (external auditors, regulators, legislators, customers, vendors, etc.) may have a significant effect on an entity's internal control process. However, they are not responsible for, nor are they a part of, that process.

Introduction – What Is Risk Assessment and Risk Management?

What Are Business Objectives?

- **"**Goals or targets that a business sets for itself, they differ according to the type of business." (Wiki Answers)

- In other words, business objectives summarize **the work you accomplish every day**.

Defining Objectives

The risk assessment thought process begins with clearly defined business objectives. What these objectives are and how they are phrased will vary, depending on the nature of the business process. The following general guidelines, however, apply to all processes and should help you define business objectives clearly.

An objective is a statement of a desired end result. In other words:

- It should describe the end, not the means to that end.
- A helpful tip for distinguishing between the means and the end result is to ask "Why do we want to do that?" The answer will usually be one step closer to the end result. For example:

  Objective: take physical inventory count annually
  "Why do we want to do that?"

  Objective: maintain accurate inventory records
  "Why do we want to do that?"

  Objective: safeguard assets held in inventory and report them accurately.

- Another tip: statements that describe specific actions, such as "record…review…verify…reconcile…" usually refer to controls. Objective statements usually begin with more general words like "minimize…improve…safeguard…ensure."

Exercise #1
Defining Objectives

Your company sells PC hardware and software through a mail-order catalogue. You have just been put in charge of the unit that takes orders over the phone. Because you are new, you want to understand just what it is you are supposed to accomplish. To do this, you ask two of the experienced telephone sales reps to join you for a brainstorming session. They come up with the following as possible objectives. Determine whether each statement is a well-defined objective for the phone-order processing unit.

Well defined objective?	**Yes**	**No**
1. Minimize cost of office space	_____	_____
2. Sell mailing list to other organizations	_____	_____
3. Keep your customer satisfied	_____	_____
4. Minimize time spent on each phone call	_____	_____
5. Be the best phone order processing unit in the industry	_____	_____
6. Provide prompt, courteous customer service	_____	_____
7. Use lowest cost shipping method	_____	_____
8. Provide 40 hours of training for each rep	_____	_____
9. Read order back to customer, to ensure orders are entered accurately	_____	_____
10. Minimize salary and benefits cost	_____	_____
11. Cross-sell other products in the catalogue	_____	_____
12. Minimize the cost of telephone equipment	_____	_____
13. Do whatever it takes to provide superior customer service	_____	_____

Introduction – What Is Risk Assessment and Risk Management?

Sources for Identifying Business Objectives

- "Charge" for Your Business Function
  - "Charges" for high-level functional areas such as academic and student affairs, clinical affairs, external affairs, finance, trusteeship and governance, strategic planning, and audit are approved by the Board of Trustees
- Operating Plan for Your Department
- Your Department's Intranet Site
- Your Performance Evaluation
- External guidance is also available for you to identify your business objectives, in the form of methodologies such as "COSO", "CobIT", and "CoCo"

THE UNIVERSITY OF TOLEDO 1872

Defining Objectives
-Control Models Can Help-

COSO, Criteria of Control Board (CoCo) and Cadbury all present three broad categories of business objectives. These categories, together with the sub-categories suggested below, can help in defining objectives for a given process.

Effectiveness and Efficiency of Operations

- Produce excellent products
- Provide excellent customer service
- Maximize revenues
- Minimize costs
- Streamline workflows
- Safeguard assets (physical, human, and information)
- Contribute to organization-wide mission and vision
- Meet social obligations (good corporate citizenship)
- Provide positive work environment for employees

Reliability of Reporting

- Internal reports used for decision making
- External reports to shareholders, regulators, and other third parties
- Both financial and operational reports

Compliance

- With applicable laws and regulations
- With internal policies and procedures

COSO

COSO Methodology

- COSO (Committee Of Sponsoring Organizations) was developed in 1992 by The Treadway Commission.

- COSO states that all business objectives can be categorized/"bucketed" as follows:

  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws, regulations, and guidelines

- More on COSO later in the course …

UNIT TWO
WHAT IS INTERNAL CONTROL? THE COSO REPORT

Overview

This unit introduces the first authoritative definition of internal control. *Internal Control – Integrated Framework* was published in September 1992 in the U.S. It was a joint product of five organizations:

American Accounting Association
American Institute of CPAs
Financial Executives Institute
Institute of Internal Auditors
Institute of Management Accountants

These five organizations formed the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. Therefore *Internal Control – Integrated Framework* is commonly referred to as "the COSO report".

Objectives

In this unit, you will:

- Learn the broad, management-oriented concept of internal control which is authoritatively accepted today

COSO

What Are Key Business Risks?

- "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." (The Institute of Internal Auditors)

- In other words, business risks are **the barriers or impediments to successfully achieving the business objectives** established by the process owner.

- Typically, a single business objective will have several business risks associated with it.

THE UNIVERSITY OF TOLEDO 1872

Ten Universal Business Risks

- Erroneous records and/or information
- Unacceptable accounting principles
- Business interruption
- Government criticism or legal action
- High costs
- Unrealized or lost revenue
- Loss or destruction of assets
- Competitive disadvantage and/or public dissatisfaction
- Fraud or conflict of interest
- Inappropriate management policy and/or decision making process

From Computer Control & Audit, by William C. Mair, Donald R. Wood, and Keagle W. Davis, Institute of Internal Auditors.

COSO

Risk Assessment Concepts and Terms

Following are risk assessment terms and concepts:

- Inherent risk
- Residual risk
- Risk categories
- Risk events
- Impact
- Likelihood
- Speed of onset
- Materiality

"Working" Inventory of Risks

External Risks:

Competitor
Regulatory
Shareholder
Environmental
Vendor/supplier
Political
Acquisition
Publicity
Capacity
Physical disaster
Capital availability

Internal Risks:

Technology
- Availability
- Accuracy / Integrity
- Confidentiality
- Efficiency

Human Resources
- Availability
- Competency
- Development
- Safety
- Integrity
- Communication
- Leadership
- Empowerment
- Rewards

Financial
- Interest rate
- Market
- Currency
- Liquidity
- Counterparty
- Credit / Concentration
- Derivative

Financial / Regulatory / Management Reporting
- Existence
- Completeness
- Accuracy
- Ownership
- Disclosure
- Valuation

Operating
- Customer satisfaction
- Compliance
- Business Interruption
- Product Development
- Brand Image
- Third party providers
- Marketing / advertising
- Business performance management
- Alignment
- Distribution

Strategic
- Strategy
- Resource allocation
- Cross business issues

Exercise #2
Defining Objectives

Select one of the following scenarios and develop a comprehensive set of six to twenty objectives.

Scenario A:

You are responsible for a county-owned public beach in southern California. The beach front is a half mile of white sand with several jagged rock outcroppings. The beach is open from 6 a.m. to 11 p.m. daily. Facilities include 8 lifeguard towers, two central complexes with rest rooms, showers, and food service, and a parking lot.

Develop objectives for managing this beach.

Scenario B:

You work as a business manager for a multi-national company. Your department has a regional business office, with six employees and one support staff, in a developing country. At this point, the office has one desktop PC used by the support staff. The six employees are all very experienced and highly competent in traditional business process management techniques. One is a good mainframe IS professional. Their training and experience in using a PC, however, ranges from little to none.

Your department has a decentralized philosophy in managing its regional offices. Your Chief Executive believes that positive customer relations are of paramount importance, and local autonomy allows the regional employees to fit into local cultural norms.

Despite her decentralized philosophy, the Chief Executive just can't stand to see this office so far behind the technological times any longer. She has charged you with bringing the office to a one-to-one employee/PC ratio.

Develop objectives for automating this office. (*Note*: these objectives should address the purpose and end result of automation for the office. They should not be your personal objectives for completing the project assigned to you.)

Exercise #3
Identifying Risks

Using the common sense approach suggested on the previous page, identify risks for the objectives you defined in exercise #2 (public beach or automating an office).

COSO

Exercise #4
Identifying Risks

Using the ten universal business risks and the inventory of risks from the previous two pages, identify as many additional significant risks as you can for the objectives you defined in exercise #2 (public beach or automating an office).

What Are (Internal) Controls?

- "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." (The Institute of Internal Auditors)

- In other words, internal controls are the policies, procedures, and **business practices in place to reduce the likelihood that identified risks will occur**.

COSO Definition of Internal Control

Internal control is a process, initiated by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Key Concepts

- Internal control is a *process*. It's a means to an end, not an end in itself.
- Internal control is initiated *by people*. It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.

COSO

What Are Internal Controls (Continued)?

- Internal controls provide reasonable, but not absolute, assurance that business risks will not be realized. Absolute assurance is very difficult, and often not cost-effective, to achieve.

- Typically, a single business objective will have several business risks associated with it, and a single business risk will have several internal controls associated with it.

Limitations of Internal Control

Internal control provides:

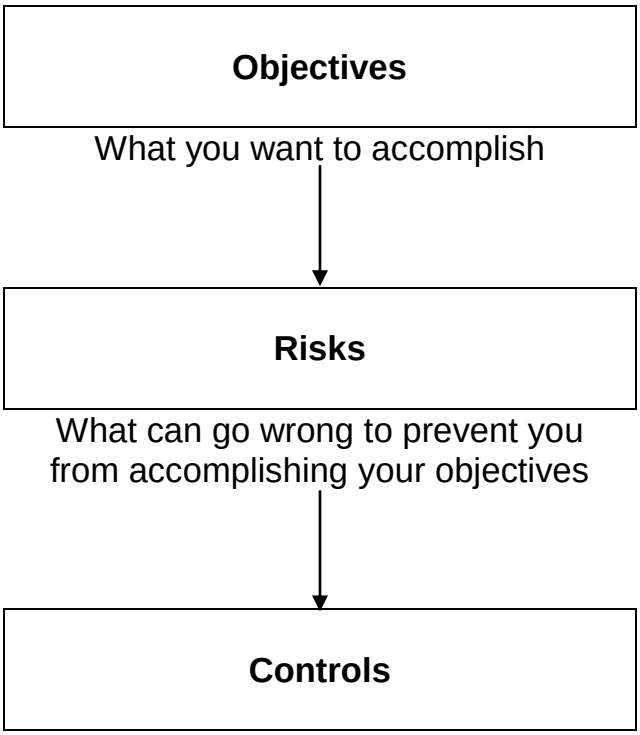
- No assurance that operational objectives will be achieved, only reasonable assurance that management will know the extent of achievement.
- Reasonable, not absolute assurance that financial reporting and compliance objectives will be achieved.

This is because of the following **limiting factors**

- **Judgment –** managers in a well-controlled organization can make bad decisions
- **Breakdowns –** people with control responsibilities may not carry them out effectively
- **Management Override –** a manager may intentionally go outside established practices for inappropriate purposes
- **Collusion –** two people can collaborate to subvert controls
- **Cost vs. Benefits –** resources are limited. Managers properly accept a degree of risk when the cost of controlling that risk exceeds the benefit

COSO

Risk Assessment Thought Process
--Simplified Version—



COSO Internal Control Framework

- The COSO framework discussed previously states that all internal controls can be categorized/"bucketed" as follows:
  - Control Environment ("tone at the top")
  - Risk Assessment
  - Control Activities (policies, procedures, business practices)
  - Information and Communication
  - Monitoring

A pictorial representation of the COSO framework is documented in the COSO cube to the right.

THE UNIVERSITY OF TOLEDO

UNIT THREE
IDENTIFYING CONTROLS

Overview

COSO and CoCo provide broad concepts of business control. In a typical process, these concepts are applied through the use of specific, concrete control tools. Control tools include COSO's "Control Activities," but they also include objective-setting, human resource practices, and any other concrete applications of any of the five components of control. In short, a control tool is anything that is used to help people stay in control of a business process.

In this unit, you will start to understand control in a more concrete way, by identifying the controls within specific business situations, and by learning some of the traditional and emerging categories of control.

Objectives

In this unit, you will:

- Learn and apply the most useful internal control categories and tools
- Learn how to identify controls in typical business situations and processes
- Learn how the nature of control changes when business processes are reengineered

Components of Internal Control

Internal control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. The components are:

- ***Control Environment*** – The core of any business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.

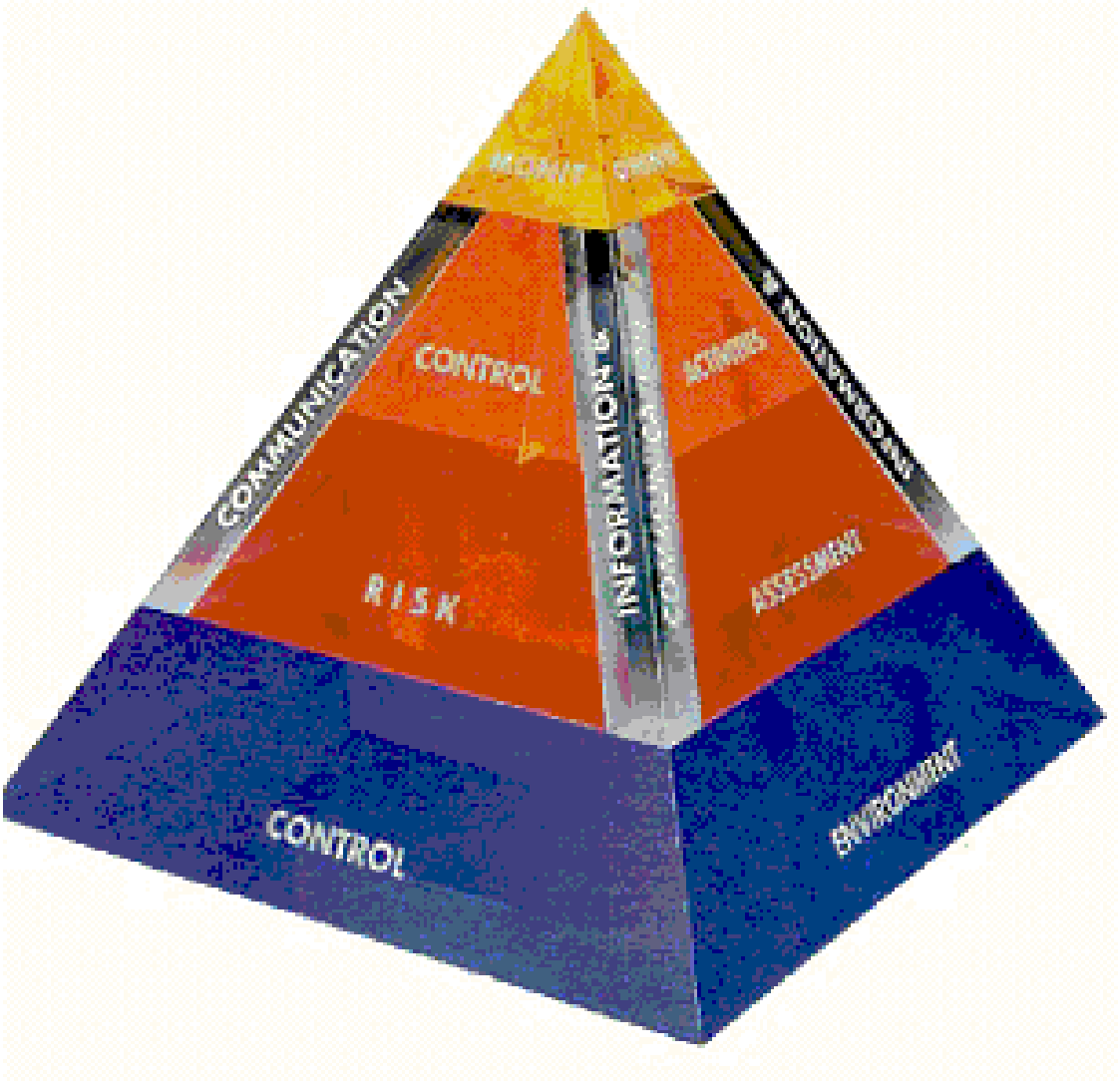
- ***Risk Assessment*** – The entity must be aware of and deal with the risks it faces. It must set objectives, integrated with the sales, production, marketing, financial and other activities so that the organization is operating in concert. It also must establish mechanisms to identify analyze and manage the related costs.

- ***Control Activities*** – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's objectives are effectively carried out.

- ***Information and Communication*** – Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange the information needed to conduct, manage and control its operations.

- ***Monitoring*** – The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

Identifying Controls



Relationship of Components and Objectives

	Operations	Financial Reporting	Compliance
Monitoring			
Information and Communication			
Control Activities			
Risk Assessment			
Control Environment			

Internal Control Components and Factors

Control Environment

- Integrity and ethical values
- Commitment to competence
- Board of Directors
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and procedures

Risk Assessment

- Objectives – entity wide
- Objectives – activity level
- Risks
- Managing change

Control Activities

Information and Communication

- Information
- Communication

Monitoring

- Ongoing monitoring activities
- Separate evaluations
- Reporting deficiencies

Some Good Control Tools

Creation of a control conscious environment

Policies, procedures, and standards

Separation of duties (authorizing, recording, and custody)

Authorization/approval

Physical and data security

Monitoring (budgets and forecasts, independent verification of performance, supervisory review, inventories)

Controlling Risks
- "Working" Inventory of Controls –

Control Environment

- Ethical "tone at the top," communicated in words and deeds
- Ethics program, including meaningful code of conduct
- Active, independent, well-informed Board of Directors
- Organization structure appropriate to entity's activities and which promote the flow of information
- Clear definition of responsibilities and accountabilities
- Delegation of authority commensurate with responsibility
- Analysis of knowledge and skills needed to perform each job; formal or informal job descriptions
- Qualified and well-trained personnel, particularly in key positions
- Frequent interaction between senior and operating management
- Appropriate policies and procedures for hiring, training, promoting and compensating employees
- Background checks for new hires, especially those in sensitive positions

Control Tools

- Written policies and procedures
- Performance standards
- Authorization/approval (with defined limits of authority)
- Reviews: budget to actual comparison, current to prior period comparison, performance indicators, project management reports, etc.
- Reconciliations
- Physical safeguards (e.g., safes, locks, access cards, dual control over sensitive assets, cameras, alarms, armed guards, identification badges, equipment labels)
- Inventory records and periodic counts
- Segregation of duties (separation of authorization, recording, and custody; at least two sets of eyes involved in every transaction).
- Operating performance reports
- Financial reports
- Supervisory review
- Inspections
- Checklists
- "Tickler" systems
- Formal compliance program, including a designated "compliance officer"
- Forms control (pre-numbered documents, filing by and verifying integrity of numerical sequence, limited access to key forms)

"Working" Inventory of Controls (cont.)

- Exception reports (e.g., receivables past due, overtime, duplicate payments, discounts not taken)
- Information systems controls:
    - Environmental controls (heat, humidity, fire extinguishers, etc.)
    - Hardware controls
    - Physical access controls
    - Data security system and confidentiality controls
    - System development methodology
    - Program development and change controls
    - Backup and recovery policies and procedures
    - Disaster recovery or business continuance plan (tested periodically)
    - Input controls – authorization, validation, error notification and correction (e.g., blocked transactions, transaction limits, error listings, field checks, self-checking digits, sequence checks, validity checks, and completeness checks)
    - Processing controls (e.g., edit checks, control totals and other programmed steps within application software, audit trails)
    - Output controls (e.g., output review, exception reports, master file change reports)
    - Software license compliance controls

"Working" Inventory of Controls (cont.)

- Inventory records and periodic counts
- Segregation of duties (separation of authorization, recording, and custody; at least two sets of eyes involved in every transaction). For example:

	Initiates	**Authorizes**	**Records**	**Reconciles**	**Custody**
Purchase of Goods	Issues Requisition **Person A**	Approves P.O. / Invoice **Person B**	**Accounting Department**	Budget report **Person C**	Receives goods **Person A or C**
Cash Receipts	Opens mail, lists checks, restrictively endorses **Person A**	Makes deposit **Person B**	**Accounting and Person B**	Bank acct. / budget report & deposits to checklist **Person A or C**	**N/A**
Payroll	Employee's time report	Approves time report and payroll data changes **Person A**	**Accounting Department**	Budget report review **Person B**	Distributes payroll checks **Person B or C**

- Operating performance reports
- Financial report
- Supervisory review
- Inspections
- Checklists
- "Tickler" systems
- Formal compliance program, including a designated "compliance officer"
- Forms control (pre-numbered documents, filing by and verifying integrity of numerical sequence, limited access to key forms)

Control Concepts and Terms

Control concepts and terms:

- Preventive control
- Detective control
- Manual control
- Automated control
- Hard control
- Soft control
- Key control

Some Useful Control Categories

Preventive — *Controls that prevent undesirable events from occurring*
Examples include separation of duties, passwords for computer programs, required authorization, and physical safeguards.

Detective — *Controls that detect undesirable events which have already occurred.*
Examples include output reviews, exception reports, reconciliations, physical inventories, and reviews.

Directive — *Controls that cause or encourage a desirable event to occur.*
Examples include policy statements, performance guidelines, training programs, and incentive compensation plans.

Mitigating or Compensating — *Controls that compensate – at least partially – for a missing or excessively costly control.*
Examples include supervisory review where separation of duties is impractical, and monitoring budget variances in lieu of transaction processing controls.

Some New Control Categories

Preventive controls "built into, not onto" the system

In a reengineered process, controls which require an employee to expend time and effort are generally viewed as "non-value added." Such activities should be eliminated or minimized. This does not necessarily mean a reduction in control. With the "enabling technology" of computers, preventive controls can often be built into the system so they function without fail 100% of the time with no human intervention.

For example, procurement card users can be prevented from making purchases which are outside policy or their individual limits. Some of the limits which can be built into each card are:

- Supplier category/SIC code
- Dollars per transaction
- Transactions per day and/or per month
- Monthly cardholder dollar limit

Any transaction that violates the predefined limits or purchasing policies will automatically be denied at point of sale.

Detective controls "deferred" to the end of the process

In high-volume, small-item processing systems, a reasonable level of control can often be achieved without time-consuming processing controls. Instead, it may be sufficient to have one control point at the end of the process, based on measurement, which will indicate that undesirable events are starting to occur. Management can then intervene and correct the situation before losses become unacceptably large.

For example, there will be some inappropriate procurement card purchases which cannot be prevented by built in limits. These would be detected by the month-end review of the transaction report.

Controlling Risks
- Key Points –

The Nature of Control is changing!

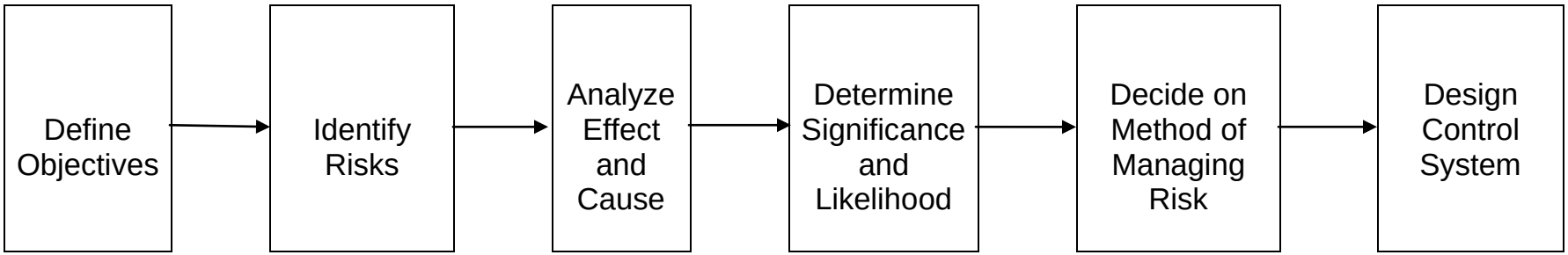
Type of Control	***Traditional***	***Modern***
Directive	Procedures Close supervision	Guidelines Training
Preventive	Approvals	System edits
Detective	Lengthy activity reports	Exception reports Trend analysis

Controls must be cost-effective!

To achieve goals, management needs to effectively balance risks and controls. By performing this balancing act, “reasonable assurance” can be attained. Being out of balance either way causes problems, such as:

Excessive Risks	***Excessive Controls***
Loss of assets	Increased bureaucracy
Poor business decisions	Increased complexity
Noncompliance	Increased cycle time
Increased regulations	Increase of non-value-added activities
Public scandals	Reduced productivity

Risk Assessment Thought Process
--Full Version—



- Desired end results
- Control models can help

- Ten Universal Risks
- "Working" Inventory of Risks
- Industry Specific Risks

- Inherent Risk

- Avoid
- Transfer
- Accept at existing level
- Reduce to acceptable level

- "Working" Inventory of Controls
- Cost-effective

Identifying Controls

"Driving to Work"

Some key business **objectives** …

- Safely get to work
- Quickly get to work
- Efficiently use a route that saves on gas
- Thoughtfully minimize disruption to coworkers through carpooling
- Carefully drive so as to avoid getting a ticket

"Driving to Work" (Continued)

Some **risks** to the objective of getting to work safely …

- Accidents
- Inattentive fellow drivers
- Obstacles in the road
- Unclear road signs
- Construction

"Driving to Work" (Continued)

Some **controls** pertinent to the objective of getting to work safely, and the risk of accidents …

- Wake up two hours before work starts
- Check driver's forecast on TV
- Maintain a three-car distance from car in front of you
- Adhere to maintenance schedule from your car's owner's manual
- Refer to MapQuest in identifying a route without construction and follow it

"Paying the Bills – Accounts Payable"

Some key business **objectives** …

- Accurately and completely making and recording cash disbursements on a timely basis.
- Minimizing processing time
- Properly authorizing accounts payable and cash disbursements.
- Developing strategic business alliances with suppliers
- Using reliable performance measurements to control and improve the process.

"Paying the Bills – Accounts Payable" (Continued)

Some **risks** to the objective of accurately and completely making and recording cash disbursements on a timely basis …

- Inaccurate transaction coding and posting errors in the accounts payable trial balance may result in non-value-added activity to correct the errors.
- Not recording purchases and cash disbursements on a timely basis
- Making payments to the wrong parties and recording disbursements for the wrong amounts because of clerical or mechanical processing errors.
- Credit and debit memos may be missing from the records because of errors like unrecorded adjustments.
- Purchase discounts may not be accurately calculated and properly recorded.

"Paying the Bills – Accounts Payable" (Continued)

Some **controls** pertinent to the objective of accurately and completely making and recording cash disbursements on a timely basis, and the risk of incorrect coding and posting …

- Use batch totals before completing the payment process for computer systems that input disbursements into a temporary file.
- Check quantities, prices, extensions and footings of invoices, accuracy of account distribution, and proper approvals prior to general ledger journal entry.
- Establish procedures to ensure period end reconciliation of the accounts payable ledger to the general ledger as well as to correct cut-off errors on a timely basis.
- Review unprocessed receiving reports and invoices periodically, and investigate and resolve them.
- Determine control totals prior to inputting invoices. Ensure computer routines reconcile this amount to the total of invoices accepted or rejected during systems processing.

Evaluating Controls

- It is not enough to identify controls that might address known risks.
- You should also be creative and identify what controls you would expect to be in place.
- Compare these expected controls to the actual controls in place and identify gaps (residual risk).
- You will then need to make a determination as to whether these residual risks should be addressed. Consider such factors as cost, compliance with regulations and policy, etc.

Evaluating Controls (Continued)

- You may not be in a position (organizationally) to address residual risks.
- As a result, you may have to formulate a recommendation for corrective action.
- Modifying the risk matrix in the following way (below) may be helpful in establishing your business case …

Business Process:						
Objective	Risks	Expected Controls	Actual Controls	Residual Risk	Recommendations	Action Plan
Several per business process	Several per objective	Several per risk				

Exercise #5
Shopping With Laura

After work on Tuesday, Laura phones her best friend, Jan. They decide to go shopping at the new mall, which is located three miles from Laura's apartment. Because Laura lives between Jan's house and the mall, they agree that Jan will pick Laura up and drive her to the mall.

Assignment:

1. Identify six of Laura's objectives for this shopping trip. Feel free to make any assumptions you want. Be prepared to state your assumptions.
2. For each of Laura's objectives, identify at least two risks.
3. When you have identified at least twelve risks, select four of these risks and design at least two controls for each of the four risks.

UNIT FOUR

INTERNAL CONTROL GAME

Overview

In this unit, you will play a "game" based on the COSO components of control. You will be given a series of scenarios which require you to decide on the best course of action. Several of these scenarios have risk management and governance issues. You will discuss each scenario with a group of your peers and arrive at a decision for your group, then compare your decision with those of other groups and with the suggested best decision.

Objectives

Upon completing this unit, you should:

- Be aware of various internal control challenges that can arise in day-to-day job responsibilities
- Have a more concrete, real-world understanding of internal control as defined by COSO
- Understand the judgmental nature of many aspects of internal control and have enhanced your own ability to form good judgments on control issues

Internal Control Game

Control Environment

Situation #1

You are a product line manager and your product line has exceeded fiscal-year budget projections by the third quarter. Your manager suggests that you should start “socking” some earnings away for next year. You are aware of Generally Accepted Accounting Principles (GAAP) regarding financial reporting.

What do you do?

A. Ask your controller to see what he or she can do to meet the demands of your manager and corporate financial reporting.

B. Ignore your manager and report earnings according to Generally Accepted Accounting Principles.

C. Tell your controller to accrue whatever the controller feels he/she can get away with so as not to run afoul of any review.

D. Call your manager and ask for more information about his/her comment and get suggestions of where your manager has concerns regarding potential liabilities.

Internal Control Game

Control Environment

Situation #2

You have just assumed the key management position in a new acquisition in a developing economy. The culture of the country in which the bulk of the business activity will occur is not consistent with your organization's values. The new business looks good on paper, but you question the ability of the current management team and staff to meet projected results. Your executive supervisor asks you to list your top priority.

What do you do?

A. Tell the executive supervisor what you know he or she wants to hear.

B. Advise your executive supervisor of the need to build a strong business team that shares the same values as the rest of the organization. Share projected implications over the short term as you replace the current team.

C. Cite the need to build the business. Stress the importance of the need to respect local customs and practices as we seek to compete in a market with different laws and cultural values.

D. Respond by saying your number one objective is to teach the acquired personnel your organization's way of doing business.

Internal Control Game

Control Environment

Situation #3

You are the country manager. The key product line in your country has been doing business in a way which is at odds with your organization's Code of Conduct. Your initial feeling is that the product line manager is the cause of this situation.

What do you do?

A. Contact geography sector management and ask for advice.

B. Ask your country controller to investigate the situation with special instructions to keep this quiet.

C. Advise geography sector management and appropriate Corporate Center management. Wait for their response.

D. Do nothing because the division is extremely profitable.

Internal Control Game

Risk Assessment

Situation #4

You are the business manager at one of the largest facilities within your product line. A key business goal is to improve margins by reducing the back office expenses. You have identified training as a cost item that could be significantly cut, but you worry about the long-term implications for your facility.

What do you do?

A. Historically you know that the corporate culture has supported cuts in training. However, you recognize the value of training key personnel, so you cut administration and production training while retaining enough to cover sales and merchant needs.

B. You refer to the annual business plan which states that training is a key initiative for the product line. You decide not to cut training and look elsewhere.

C. You contact your product line human resources manager and ask for a recommendation on how to cut training costs while still meeting critical business needs.

D. You look for inexpensive local training that might not be appropriate but makes it appear that you are supportive of training and allows you to meet your cost objectives.

Internal Control Game

Risk Assessment

Situation #5

You are on the strategic management team responsible for identifying the future direction of the business. You question the abilities of both the finance and information technology functions to support the growth of the business. You are especially nervous about the lack of professionals with effective communication and technical skills in the regions projecting the bulk of the growth.

What do you do?

A. You ask that your concerns be documented in the team's proposal.

B. You suggest that the team solicit key Corporate Center management input to better define the risk.

C. You ignore the feeling by rationalizing that this situation occurs in most organizations.

D. You solicit input from key product line managers who are not on the team and discuss your findings and concerns with the management team.

Internal Control Game

Control Activities

Situation #6

You are the plant manager at the largest facility in your product line. Your product line has been scheduled to undergo Business Process Reengineering (BPR) in three months. You have traditionally relied on certain key controls such as maintaining separation of duties and having key accounts reconciled. Your facility manager asked you to state your number one issue associated with the pending BPR project.

Which of the following would be your highest-priority issue?

A. Training – Your concern is that the aggressive timetable, coupled with other time demands placed on your staff, will result in your staff not being adequately trained.

B. Resources – Your concern is that with a reduced staff, traditional control activities, such as maintaining adequate separation of duties and reconciling key accounts, will be impossible.

C. Standards – You feel strongly that minimum control activity standards should be in place before undergoing BPR.

D. People – Your concern is morale and how people will react to change. You worry that key personnel will leave or that you will not be able to find jobs for them after BPR.

Control Activities

Situation #7

You are a regional manager. You have just received a wire from your region's information technology (IT) manager outlining the timeline associated with a major system development project in your region. This project appears to be on line with corporate IT initiatives. What best describes your role as this project progresses?

What do you do?

A. Given that this is a complex and technical project, you rely on your region's IT manager to monitor the progress. You assume you'll be advised when appropriate.

B. You ask for a complete overview of the project scope as it relates to people, customers, costs, and training. You will respond based on input.

C. As stated in "A" above, you recognize your limitations in this area; however, you feel you should monitor the progress on this project given the capital spending required to complete the project. You decide to mentally keep track of the progress using the monthly reporting process.

D. Given the impact on a major product line within your region, you clarify roles and responsibilities within the matrix to ensure that key control activities are properly addressed.

Internal Control Game

Control Activities

Situation #8

You are a trading manager overseeing the trading activities of 10 traders and back office personnel. Given the global trading patterns associated with your line of business, some of the trading occurs outside of the normal workday. Recently, the monthly comparison of the budget to actual trading results has shown significant differences. Turnover in the accounting staff has been quite high, and you are not very confident of your accounting manager's abilities.

What do you do?

A. Participate in the upcoming monthly reporting process by offering your assistance in reconciling budget to actual. Get to the level of detail you need to ensure things are accurate. Contact your supervisor alerting him/her to the issue and ask for suggestions as to the best course of action.

B. Go directly to the product line controller outlining your concerns relating to the financial staff's recent performance.

C. Investigate whether or not the key controls associated with trading are being followed by your traders and back office personnel.

D. Nothing. It is the job of the financial manager and staff to reconcile the differences with adequate documentation as to causes.

Internal Control Game

Control Activities

Situation #9

You are a production engineer at a large site. Recently, yield reports have been indicating a potential shrink problem. What is troublesome is that your facility has had little turnover of personnel, no major process or systems changes and historically has been within acceptable yield ranges. While your team can think of numerous areas to begin investigating, which of the following areas would you begin reviewing for probable cause?

What would you do?

A. Hiring – Employee background checks, training.

B. Production/Shipping and Receiving – Weights, sampling, reports, segregation of duties.

C. Accounting – Reports, segregation of duties.

D. Security – Information systems, plant, office.

Internal Control Game

Information and Communication

Situation #10

You are an experienced merchant but are new to your current product line. Over the last month, you have observed behavior which is not consistent with your organization's Statement of Guiding Principles or with the policies and procedures you are familiar with from your previous product line. The management team of your new product line has embraced the concept that everyone must "be part of the business team," and you don't want to appear to be a maverick.

What do you do?

A. Nothing. While the corporation promotes values and principles, it does not offer support for a new person challenging the current business team.

B. Communicate your concerns to either your human resource manager or controller, seeking guidance.

C. Using tact, discuss the situation with the product line manager to seek a better understanding.

D. Anonymously advise the Business Conduct Committee or the appropriate attorney at corporate headquarters.

Internal Control Game

Information and Communication

Situation #11

You are the product line manager and it is the fourth quarter of the fiscal year. A recent unforeseen event could result in your business unit not making budget for the year; therefore, incentive bonuses are in jeopardy. A serious quality problem may exist with one of your key customers. However, it will be weeks before any conclusions can be reached. Next week your sector management team is flying in for a routine visit.

What do you do?

A. Advise only your supervisor and let him/her handle all communication.

B. Wait until sector management visits and advise them accordingly.

C. Nothing. Until all the facts of the situation are known, it makes little sense to stir up trouble.

D. Immediately inform all impacted parties – e.g., Law, Public Affairs, Corporate Environmental, Health and Safety, Food Safety – as well as sector management.

Information and Communication

Situation #12

You have been named the new vice president of administration of a recent acquisition. You are the only employee from the acquiring organization on the management team. The acquired company has had a very hierarchical structure. It relied on extensive controls and approvals.

Determine which of the following areas you would rank as your top priority.

A. People – Most of the people retained are very loyal to the old company. They are proud of what they accomplished, and some are not very excited about being acquired by your organization.

B. Systems – A major justification for the acquisition was the belief that your organization could improve the efficiency of the assets acquired. Coordinate efforts to eliminate costs.

C. Performance – Conduct a review of performance for all business processes.

D. Structure – Integrate the acquired business into your organization's network of reporting (e.g., budgeting, monthly reporting).

Internal Control Game

Monitoring

Situation #13

You are a manager. Recently you have been invited to speak at a trade association seminar. During the question-and-answer segment, you are asked the following question: "Who performs the primary monitoring function within your company?"

Which of the following monitoring categories best represents the answer you want to give?

A. Internal and External Audit – Internal Audit's primary responsibility is to assess the system of controls. The annual examination of the financial statements by external auditors represents to the shareholders and lenders that the financial statements are accurate as of May 31, 20xx

B. Customers – Our customers are our best form of monitoring. If we produce goods and services as required by our customers, we must have a good system of control.

C. Financial/Accounting – A traditional role of the financial job family is to ensure assets are safeguarded. One of the key roles of a controller and his/her staff is to ensure controls are adequate.

D. Individuals – Everyone has a role in monitoring as it is a key component in ensuring we are continually meeting the needs of our customers and controlling our business risks.

Internal Control Game

Monitoring

Situation #14

Your friend recently read another newspaper article about a major multinational corporation with a great reputation suffering a major loss due to a lack of controls. Your friend asked whether you think it could happen at your organization.

What do you do?

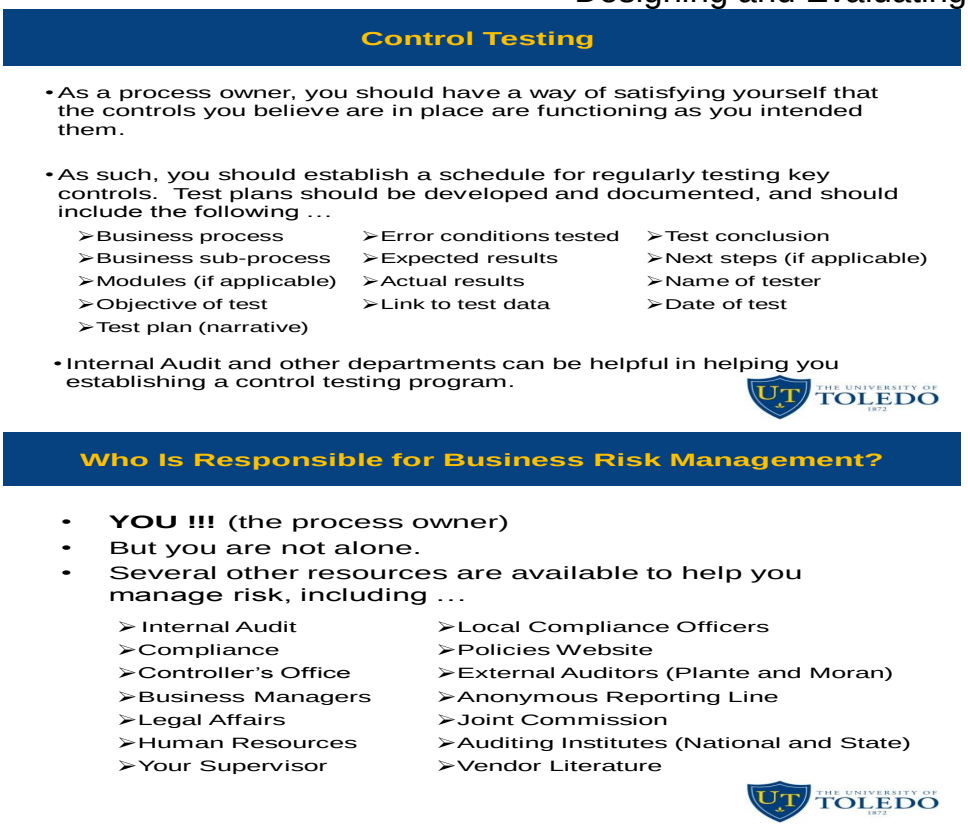
A. You acknowledge that your organization is a corporation with a solid history of success. You state that a company doesn't get that big without good controls and good people. You emphasize that controls add value to a business by ensuring that it is able to continue doing business in the future.

B. You reply that in your capacity you keep a daily focus on that issue. You state that no system of internal control is foolproof. However, you conclude by saying that your board of directors and senior management has set the proper tone at the top and that every employee shares in the responsibility.

C. You respond by saying that it is a good question. Hopefully someone is addressing whether or not it could occur.

D. You comment about the changing world and the pressure to compete globally as well as locally. You conclude by asking your friend a question. "If we want our employees to be creative and entrepreneurial, are we better off telling them what to do or telling them what not to do?"

Designing and Evaluating Controls



UNIT FIVE -- DESIGNING AND EVALUATING CONTROLS

Overview

In this unit, you will work through a disciplined thought process which will enable you to design an appropriate, cost effective set of controls for any business process. You will also learn to use the risk/control matrix, a tool based on the risk assessment thought process you learned in the last unit. The risk/control matrix is increasingly becoming the primary tool of progressive departments.

Objectives

Upon completing this unit, you will be able to:

- Clearly define the objectives for a business process
- Identify the risks to achieving each objective
- Determine the cause and effect of each risk, as well as the likelihood and significance of it occurring
- Decide on the best method for managing each risk
- Design cost-effective controls to minimize risks
- Understand the difference between control adequacy and control effectiveness, and why this is an important distinction.
- Be able to use the risk/control matrix as a tool to evaluate the adequacy of control systems.

Improving Risk Identification Skills

In many situations, it is sufficient to identify "what can go wrong" without worrying about how this is phrased. But in other situations, it is helpful to clarify our thinking by indentifying both the *cause* and the *effect* of the risk.

- The *effect* is the ultimate consequence, the harm that is done or opportunity lost when the risk is realized. It should be quantified if possible. If it is not quantifiable, it should be expressed in specific and concrete terms.

- The *cause* is the reason why the risk might be realized.

For example, we might think of the risk, "being out of compliance with OSHA regulations." This can be clarified by identifying the effect and cause:

Effect: The specific penalties for noncompliance with the regulations. These may include fines; imprisonment (which can be quantified in dollars and years); and bad publicity (cannot be quantified but may be the most significant effect).

Cause: Employees do not understand what is needed to be in compliance, or they don't consider it important.

Having identified the effect of noncompliance, we can go on to the next stage of the thought process and identify its significance. This will allow us to prioritize it compared to the other risks we've identified, and determine whether possible controls are *cost-effective*.

Having identified the possible causes of noncompliance, we are better able to design controls which effectively prevent or detect the risk.

Assessing Risks

Once we have clearly identified the risks in a business process, we need to assess them. That is, we need to determine both the *significance* and *likelihood* of each risk. This will enable us to devote most of our effort to the most important risks and to determine how much control is necessary and cost effective for each risk.

Risk assessment is a common sense process. For our purposes, the following simple criteria and matrix are sufficient.

Key point: In evaluating risks, consider inherent risk, i.e., do not consider the processes or controls in place to manage the risks.

Evaluation criteria:

Category	Likelihood	Significance
LOW	Unlikely risk will occur	Probably will not materially impact the attainment of the objective if the risk occurs
MEDIUM	Somewhat likely risk will occur	May impact the attainment of the objective if the risk occurs
HIGH	Likely risk will occur	May significantly impact the attainment of the objective if the risk occurs

Assessing Risks (cont)

Evaluation matrix:

	High			
LIKELIHOOD	Medium			
	Low			
		Low	Medium	High

SIGNIFICANCE

Risk/Control Matrix

PROCESS: Employee Expense Report Reimbursement Process

Objectives	**Risks**	**L/S**	**Controls**	**Control Design Adequacy**
Financial Reporting:				

Designing and Evaluating Controls

PROCESS: Employee Expense Report Reimbursement Process

Objectives	**Risks**	**L/S**	**Controls**	**Control Design Adequacy**
Regulatory Compliance:				

Designing and Evaluating Controls

PROCESS: Employee Expense Report Reimbursement Process

Objectives	**Risks**	**L/S**	**Controls**	**Control Design Adequacy**
Safeguarding Assets:				

Designing and Evaluating Controls

PROCESS: Employee Expense Report Reimbursement Process

Objectives	**Risks**	**L/S**	**Controls**	**Control Design Adequacy**
Operational Efficiency:				

Managing Risks

Once we have clearly identified and assessed the risks facing our business process, we can decide how to manage each risk. We have four possibilities.

Avoid

Examples:

Transfer

Examples:

Accept at existing level

Examples:

Reduce to acceptable level

Examples:

Cost-Effective Control

Situation A: Family Car

Objective: maintain adequate fuel supply

Risk: loss of time and unpleasant experience walking or hitching a ride to the nearest gas station

Control: gas gauge

Is this adequate control, given the risk?

Situation B: Boeing 767

Objective: maintain adequate fuel supply

Risk: loss of hundreds of lives

Controls:

1. Fuel quantity processor: a computer which uses a complex electronic network to measure the volume, weight and temperature of fuel in each of the twelve fuel tank compartments.

2. The fuel quantity processor is “dual channel.” Two separate channels run on dedicated power sources. If one channel is not working properly, it automatically switches to the other channel. Thus, it provides a redundant control.

3. If there is any question about the functioning of the fuel quantity processor, mechanics measure the fuel before the plane takes off. This measurement is input to the flight management computer system. This additional system measures the fuel flowing through the line to the engines, so it calculates the amount left at any moment.

Is this adequate control, given the risk?

Adequate Control

1. In May 1983, a fuel quantity processor malfunctioned due to a poorly soldered connection which allowed some but not enough electricity to pass through. This prevented the system from switching to the other channel, and the processor stopped working altogether.

2. Measuring the fuel involves taking readings of fuel depth at multiple positions, factoring in how level the plane is sitting on the runway – front to back and side to side – factoring in the temperature and therefore the specific gravity of the fuel, and making conversions between weight and volume measures – all of which is done manually.

3. In 1983, Canada was converting from English to metric measurements.

4. In other large planes, three pilots were required. The third, or reserve pilot was responsible for the accuracy of refueling. But the 767 was a new plane, and the sophisticated computerization made the third pilot unnecessary, per the FTA. To remain competitive, Air Canada convinced its regulators to allow it to fly without the third pilot.

5. The accountability for refueling passed to the mechanics. However, they had not yet been rigorously trained.

6. The pilot and co-pilot were concerned, so the co-pilot questioned the mechanics and had them re-measure the fuel. But both were confused between the metric and English systems and used the familiar sounding fuel conversion factor of 1.78 to convert the measured liters to kilograms. Unfortunately, 1.78 converts liters to pounds (at the specific gravity they measured). The correct conversion factor for kilograms was .8.

The result was that the plane left the ground with the flight management system reporting an excess of fuel, and this system reported more than half the original amount left in the tanks when the plane ran out of fuel halfway between Montreal and Winnipeg.

Control breakdowns:

- Unclear accountability
- Lack of training (resulting from unclear accountability)
- The effect of change (new plane, new procedures, English to metric)

- Summarized from *Freefall*, by William Hoffer and Marilyn Mona Hoffer, St. Martin's Press, 1989.

Scenario #1
New Business Manager

Assignment: underline all controls in the following scenario (regardless of whether you think they are effective).

Peter is a new business manager. When he got to work Monday morning, his Manager introduced him to his co-workers. She then brought him to the supply cabinet and gave him the paper, pencils, etc. he would need. She then brought him to her office, where she gave him his assigned notebook computer and portable printer. She had him sign a log to acknowledge he received it. Finally, she showed him his desk and told him to make himself comfortable until 9:30, at which time he was scheduled to attend an orientation session at Human Resources.

At the orientation session, he was asked for proof of citizenship. The benefit programs were explained, and he was given a manual on each program. He was shown a video in which a trainer from HR explained the organization's vision and values. He was given a copy of the code of conduct and asked to sign an acknowledgement that he is complying with the code, which he did immediately.

After the orientation session he returned to his office, where his co-workers were waiting to take him to lunch. During lunch, they had many questions for him and told him a lot about themselves and how they work together. It was a very good "get to know each other" session.

After lunch, his Manager brought him two thick manuals. One was the Technical Business Manual; the other was the Administrative Manual. Together, they contained all the policies and procedures which would apply to his job, together with explanatory material. She told him he would have the rest of the week to familiarize himself with the information in the manuals and the office surroundings. The next week he would start on his first project. She invited him to come to her with any questions about the information in the manuals. Twice that week she stopped by to ask how he was doing.

First thing the next Monday morning, Peter reported to his Manager's office. She walked him over to the department where he would be working on his first project.

The lead employee gave Peter a ten page work program and explained that it was quite detailed, because he knew Peter was brand new and could use detailed directions. He introduced Peter to the department supervisor Peter would be working with the most and told Peter to come to him (the lead business manager) with any questions. He also told Peter to give him the documents for each program step as soon as they were completed, so he could give Peter timely guidance.

Tuesday morning, Peter handed in the three-page documents for his first completed program step. An hour later, he got back four pages of “points” and was told to clear them all before continuing with his other program steps.

Scenario #2
A Day in the Life of Tom

Assignment: Underline all controls in the following scenario.
Circle anything that might be a control weakness.

Tom has a clerical position in a small regional processing center. His typical day starts with filing the paperwork for the previous day's sales orders and paid invoices.

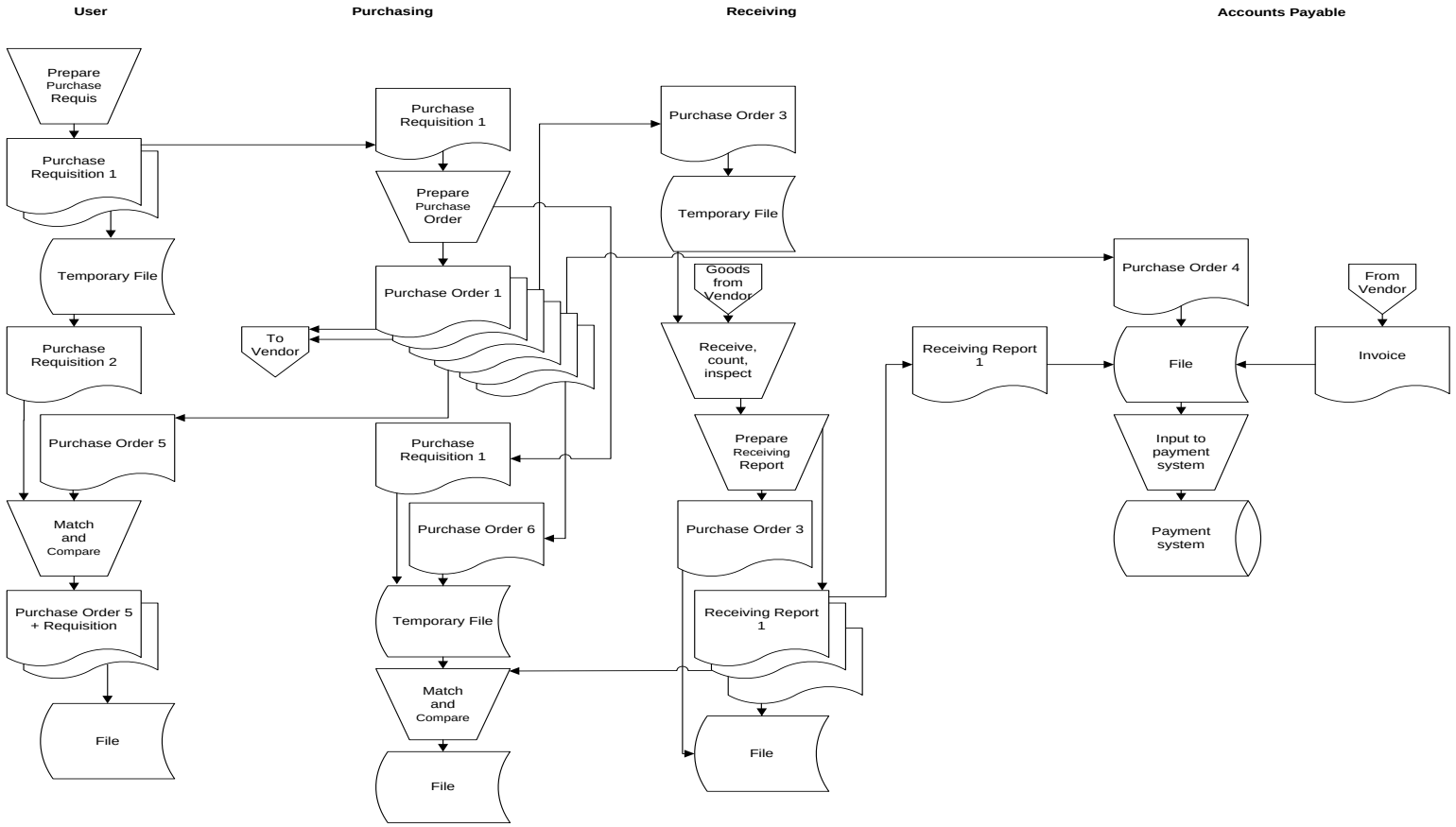
When the morning mail arrives, he opens all pieces that are not addressed to a specific person and distributes them. He gives all invoices directly to the accounting supervisor, who distributes them to the accounts payable clerks. For each payment that comes in, he records the amount of the cash or check on a list and restrictively endorses the checks. He gives these to Sally, the receptionist, who uses the lists to make out a deposit slip and deposits the funds at the end of the week. After Sally makes the deposit, she gives the receipt to John in the Accounting Department to make out the general ledger entry. At the end of the month, Sue in Accounting reconciles the general ledger to the bank statement.

Tom is also responsible for maintaining the office supplies. Each day he looks through the supply cabinets to see if anything is getting low. If it is, he fills out a requisition form and delivers it to Jan, who is in charge of purchasing.

Tom covers for the receptionist during her lunch and breaks. If no calls are coming in, he sometimes performs simple accounting tasks like updating depreciation schedules to keep productive. At other times, he does homework (he is taking night classes) or reads novels.

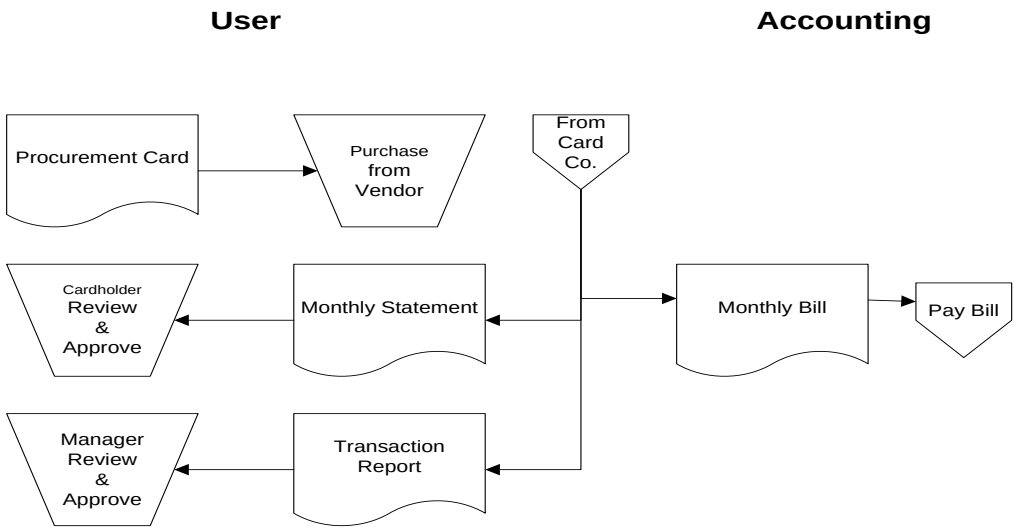
At 4:50 each day, he brings the various items that need approval to the manager of the processing center. There are anywhere from 20 to 80 of these items in a typical day. Rather than have numerous interruptions, the manager likes to sign them all at once. When he is finished, Tom puts the approved items in a drawer to be filed or distributed the next morning. He locks the drawer and, since it is now 5:00, goes home.

Scenario #3
Purchasing Flow Chart

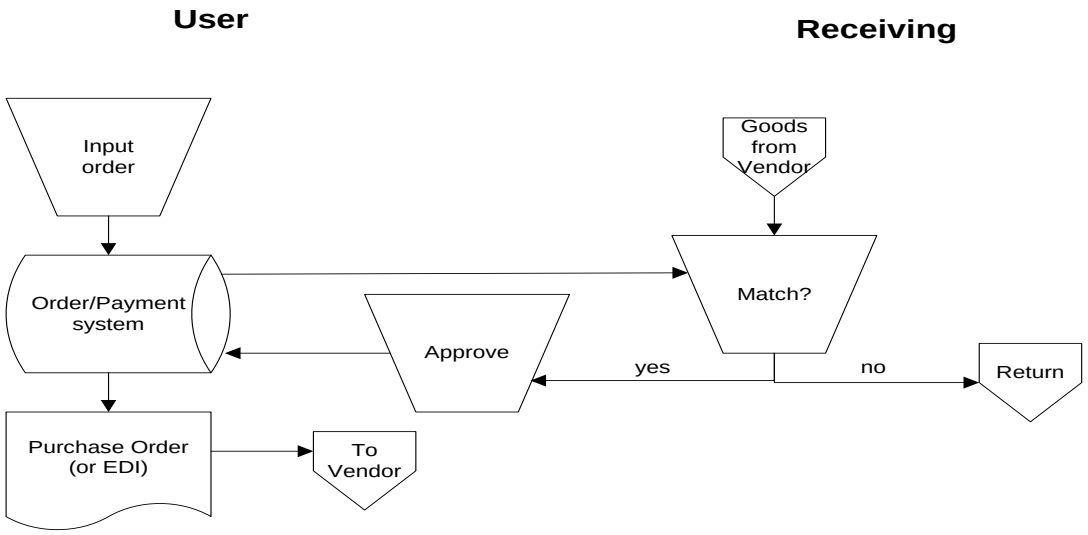


Scenario #4
Purchasing Flow Chart after Reengineering

Purchases <$1,000:



Purchases >$1,000:



Exercise #6
Controlling Senior Management

You are a business manager assigned to review a process which is directed by a committee of senior executives. The process is fairly new to your industry and technically complex. Your initial meetings with the employee who provides staff support for this committee and your review of available documents give you the impression that the process has no clear direction, and little progress has been made to date, although the committee has been meeting for over a year.

In particular, the meeting minutes give the impression that topics arise, are discussed – often insightfully – then dropped as the discussion moves on to a related topic. After 45 – 60 minutes of interesting philosophical discussion, the committee adjourns, with no real decisions made.

The committee staffer seems highly competent. He is well versed in the current state of the process within your industry from reading the available literature, attending conferences, etc. He admits to being a little frustrated by the lack of direction from above, but feels he is making reasonable progress in developing the analytical tools needed to manage the process. He says others in your industry are quite a bit further along the path they have chosen, and he could be further along if he had a definite path to follow. But he is willing to accept the management style. Perhaps, he says, he should see this as an opportunity to set the direction himself. The analytical tools he is developing will unavoidably lead the organization in a certain direction.

Required

1. *Is this organization likely to "get it right the first time" with this new process? What is lacking?*

2. *Design a control or set of controls which will influence senior management to behave more effectively.*

Exercise #7
Wahoo University

Laura Smith is a new employee in XYZ Department at Wahoo University. It is her first day on the job and her Supervisor offers to introduce Laura to people in the department.

First, Laura meets the office Secretary who informs Laura after she meets everyone in the department, she needs to go down to Human Resources and fill out a bunch of forms. The Secretary says to Laura, "Don't worry about reading any of it, just tell them you want automatic everything and you can be back in time for us to take you to lunch."

While walking down the hall to meet the next person, Laura asks her Supervisor about department policies and procedures, especially those that pertain to her job. The Supervisor informs her that there are not any department policies and procedures and that she should just look around her office and figure out the way the previous guy did her job. The Supervisor says to Laura, "I think we have something called *Regents' Rules and Regulations*, but I've never seen them. If you have a question, ask me and I'll call Frank Wise. He's been with this place for years and he knows all the ways to get around bureaucracy around here."

Next, Laura meets the office Accountant. As she walks into the Accountant's office, she notices that he is playing a golf game on his computer. Obviously embarrassed, he explains that he just got the game from a guy in Information Resources. As he exits the program, she notices that a Federal income tax return pops up on the screen. He explains that he does a few personal income tax returns on the side to make a few extra bucks. "After all," he explains, "they don't pay a person what he's really worth around here."

Next, Laura meets the Assistant Director. He requests a private meeting with Laura to introduce himself to her. While in the office, he asks, "Well Laura, I noticed that you aren't wearing a wedding ring. Are you seeing anyone right now?" Surprised by his question, she doesn't say anything. He says, "You are a very attractive woman and I like to encourage all our people to get to know each other inside and outside the office. I look forward to our working together and if you ever need anything, just come by and see me."

After meeting several other people in the office, she meets the Director of the department. He seems very nice and apologizes for not being able to go to lunch with her and everyone else. He explains that he has made lunch plans to meet and old buddy who is bidding on one of the department's requests for proposal (RFPs).

After filling out the forms in Human Resources, Laura returns to the office and finds that everyone is waiting for her to go to lunch. Laura explains that she brought her lunch and that she needs to go cash a check to go out for lunch. The office Secretary says, "Don't worry, Laura, just get $20 out of the petty cash fund for your lunch. It's an unofficial benefit for first day employees. I'll write it up as a 'miscellaneous expense.'" Laura is stunned; she does not know what to do.

Required

1. *Underline everything in this case study that contributes negatively to the Department's control environment.*

2. *What does this department's control environment communicate to Laura?*

3. *Assume you are a business manager called in by the Director of this department to do a consulting review. He is concerned that department productivity seems to be lagging behind that of other departments, and several things he observed recently have caused him concern. These include questionable items on employee expense reports, delays in producing the department's monthly financial reports, and negative comments made during "exit interviews" with employees who left the department. He said he is sure there are no serious problems, and a couple of years ago he wouldn't have been concerned. But with the Regent's new "accountability kick" (in response to some highly publicized University-wide control breakdowns) he wants to be sure his department doesn't get caught "with its pants down."*

   You obtained the above information by interviewing Laura, the department's newest employee. Other interviews confirm the impression she gave you. What recommendations should you make to the Director to improve the control environment? In other words, design an effective control environment for this department.

Exercise #8
Improving Risk Identification Skills

Try to identify the following risks more precisely by clarifying the effect and cause. Feel free to make any assumptions you like about the situation.

1. Expense reports lack proper supporting documentation.

   Effect:

   Cause:

2. Sales representatives may grant excessive or unnecessary discounts to customers.

   Effect:

   Cause:

3. Division performance may be misrepresented to senior management in performance reports.

   Effect:

   Cause:

Exercise #9
Improving Risk Identification Skills

Select three of the risks you've identified for the public beach or automating an office. Define them more precisely by identifying their cause and effect. Be prepared to explain whether and how this greater precision will help you design effective controls for these risks.

Exercise #10
Assessing Risks

Assess the likelihood and significance of the risks you've identified for the beach or office automation exercise. Considering both the significance and likelihood of each risk, give the risk an overall ranking of high, medium, and low. Record the risks below.

High Risks:

Medium Risks:

Low Risks:

Exercise #11
Designing Cost-Effective Controls

Business Process: Employee expense reimbursement

Objective: Prevent reimbursement of fraudulent or inappropriate expenses.

Rate the following controls high (H), medium (M), or low (L) in terms of their cost-effectiveness.

___ 1 Review all expense reports (i.e., accounts payable traces all expense items to original receipt and recalculates).

___ 2 Managers review monthly cost center report (actual expenses compared to budget and to prior year)

___ 3 Require receipts for all expenses, regardless of dollar amount

___ 4 System flags large/unusual items (e.g., daily expenses >20% over the average for a given travel location).

___ 5 Review all expense reports identified by system flags.

___ 6 Review 10% of all expense reports on a random basis

___ 7 Senior management review of expenses by cost center (actual expenses compared to budget and to prior years)

___ 8 Provide written guidelines on what expenses are allowable.

___ 9 Terminate any employee caught cheating on an expense report

___ 10 Require manager approval on all expense reports

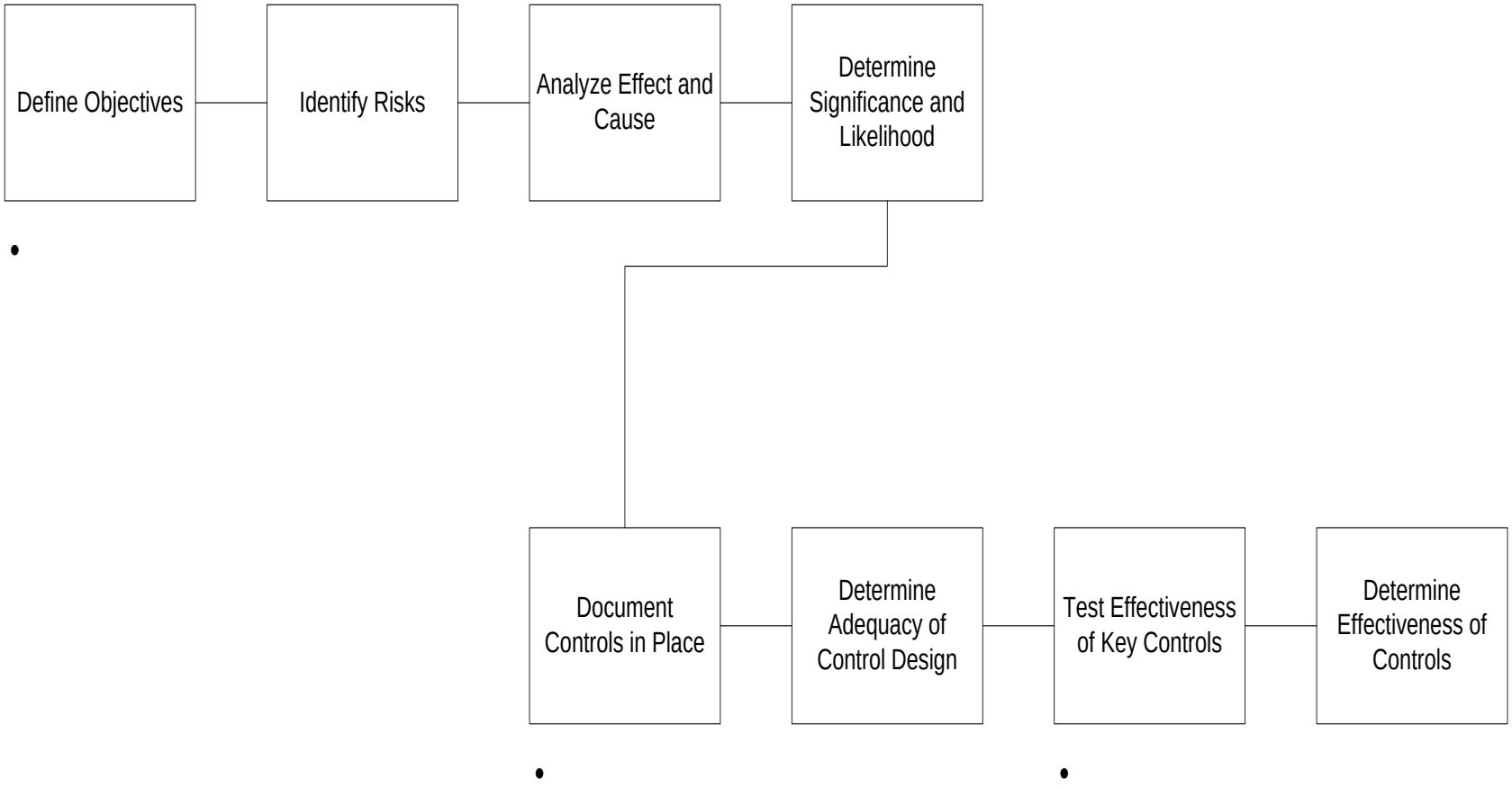
___ 11 Require manager approval on all expense reports >$200

___ 12 Creation of a control conscious environment

Exercise #12
Controlling Risks

Design appropriate, cost-effective controls for the risks you've identified as "high" for the public beach or office automation exercise.

Control Evaluation Thought Process



Risk / Control Matrix
--One Version—

Objectives	Risks	L/S	Controls	Conclusion on Design Adequacy	Effectiveness Tests
Operational: **Financial:** **Compliance:**					

Portions of a Completed Risk/Control Matrix on the Customer Service Process

PROCESS OBJECTIVE: The organization's vision and commitment to quality customer service has been clearly established and communicated to personnel. *Category of Objective:* Operational	Risk: H/M/L	Controls Adequate Y/N	Tested at:
Risks:			
• The organization is not committed to quality service and imparts this message to our customer service personnel, resulting in poor attitudes towards service and poor service	H		
• Service quality is lower than our competition, resulting in inability to compete.			
• Back office support personnel do not have the same service commitment as front-line customer service personnel	M		
• Front-line personnel do not receive the quality of service from support personnel inhibiting the provision of quality service to our customer	H		
• Service expectations within and throughout the organization are inconsistent from one area to the next.	M		
Control Activities:			
a. The corporate vision/mission statement has been written and issued to all employees by the President. The commitment to providing the best possible service was stated in the cover letter from the President to each employee. The vision/mission statement clearly states the corporate vision, mission, values and style in terms of customers, shareholders, employees and communities.			
b. The Employee Handbook includes the Corporate Vision/Mission statement. This is also distributed in new employee orientation.			
c. Corporate Vision/Mission statements are posted in all departments/offices.			

Designing and Evaluating Controls

	Risk: H/M/L	Controls Adequate Y/N	Tested at:
d. Periodically executive management, CEO and President issue memos to all employees stressing the importance of quality service. The importance of this is commented on in the quarterly corporate update video tapes and presentations to management and employees.			
e. The corporation has established a "Customer First" award program to recognize employees who have gone beyond the call of duty to serve customers. This includes both front-line and back office employees.			
f. Customer First brochure/evaluation forms have been developed and are conspicuously placed within the retail offices where customers can obtain and complete evaluating/communicating the quality of service they received.			
g. Annually, CRAs (critical result areas) are set by management for each employee. These CRAs establish performance areas and expectations against which the employee's performance is evaluated. The CRAs are reviewed with the employee by the manager and initialed by both the manager and employee to indicate their understanding.			
h. Service is defined within the organization as identifying and fulfilling needs of our customers. The Fast Forward sales program is based upon an integrated sales/service philosophy and approach. Refer to the sales management risk/control matrix for controls to assure customer needs are being identified and met by the organization.			
Control Assessment a. Overall Design of Controls: ***The design of the controls provides reasonable assurance that the control objective will be achieved.*** b. Overall Effectiveness of Control Activities: Testing of effectiveness and assessment will be performed in each individual branch examination. *Observations:* ***No opportunities for improvement noted.***			

Designing and Evaluating Controls

2. PROCESS OBJECTIVE:	Risk: H/M/L	Controls Adequate	Tested at:
Customer complaints are handled properly, timely and resolved to the satisfaction of the customer.		Y/N	
Category of Objective: Operational			
Risks:			
• Customer complaints or problems may not be handled timely and to the satisfaction of the customer resulting in a lost or dissatisfied customer.	H		
• Customer problems may not be resolved resulting in a lost or dissatisfied customer.	M		
• Negative publicity may result from poor handling of customer problems resulting in harm to the company's image and reputation in the marketplace.	L		
• Complaints or problems may not be communicated to the right areas so that the internal problems resulting in the issue can be corrected to avoid future complaints from other customers.	H		
• The success in recovering from customer malpractice situations is not known or monitored.	M		
• The volume and magnitude of customer complaints is not known or tracked to identify internal problems or assess service quality.	M		
Control Activities:			
a. The focus of controls regarding commitment and capability mentioned in previous process objectives is to "do it right the first time" in order to avoid problems.			
b. Each employee is responsible for the proper handling, resolution and follow-up on any complaint they receive. This responsibility is communicated through Front-line Customer Service Training.			
c. A record of complaint letters received by the Executive Offices is maintained. These complaints are forwarded to the appropriate area of the company for research and resolution. A reply and summary of the issues and resolution is requested by the Executive Offices from the area assigned responsibility for follow-up and resolution.			
d. The Customer First Brochure comments returned by customers are returned to the State Director and Area Manager for review. They follow-up as appropriate to resolve *or* assure the issues have been resolved.			

Designing and Evaluating Controls

	Risk: H/M/L	Controls Adequate Y/N	Tested at:
Control Assessment: a. Overall Design of Controls: ***The design of the controls does not provide reasonable assurance that the control objective will be achieved.*** b. Overall Effectiveness of Control Activities: Testing of effectiveness and assessment will be performed in each individual branch examination. Testing of each branch's handling of complaints will be performed in individual office reviews. *Observations:* Customer complaints may be received in writing from customers or mentioned to an employee either in person or over the phone. The complaints could be received by any number of employees. Therefore, it is difficult to record and track the volume or resolution of the complaints. There is no stated policy or practice regarding the handling of customer complaints. Most complaints received are not recorded, tracked and reported in order to identify causes for the problems.			

A Word about the Internal Audit Department

- **Our Charge:** "... oversight and continuous improvement of fiscal and other controls for the University and insures that the fiduciary responsibility of the Board is carried out." "…insure that the highest ethical and legal standards are met."

- In other words, independently and objectively evaluate the effectiveness of the risk management activities of the process owner.

- "Lines of Business"
  - ➢Financial and operational audits
  - ➢Information Technology audits
  - ➢Compliance reviews
  - ➢Control Self-Assessments
  - ➢Business Process Improvement
  - ➢Commercial contract reviews
  - ➢Best practice reviews
  - ➢Ethics investigations
  - ➢Data privacy audits
  - ➢Continuous controls monitoring

THE UNIVERSITY OF TOLEDO 1872

Case Study
Expense Report Reimbursement Process

You are responsible for evaluating the design and operation of controls over the employee expense report reimbursement process for the RLC Regional Office.

During the planning meeting, your scope was limited specifically to processing expense reports at the regional office level. Ignore processing that occurs beyond rendering the payment. Do not consider risks associated with retrieving stored documents in the event of a review by a regulatory body. Do not consider any aspects of the annual planning process relative to expense control.

You've reviewed the prior documents and applicable procedural manuals. You've had discussions with the lead employee and several employees involved in the process. The information you uncovered follows.

Designing and Evaluating Controls

Assignment: In the real world, you would want to work through the analysis in partnership with your internal customer. But in the classroom, this is not feasible. So you will have to perform the analysis by brainstorming with your group, making assumptions if the information provided does not answer all your questions.

Define objectives, identify and assess risks, and evaluate the control activities over each objective. (You can use the blank risk/control matrix forms which follow the information to record your work.)

RLC has several hundred employees within several major departments: Sales, Manufacturing, Distribution, and Controllers (the office out-sourced Human Resources years ago). The Controllers department is responsible for reviewing and approving each disbursement for compliance with Company and IRS requirements. The disbursements are then batched and forwarded to the Company's Data Center for entry into the Accounts Payable system and for payment.

RLC's Controller, Sam Eversharp, recognizes expenses as a high risk area and has set specific requirements. For example, all expense reports are required to be accompanied by original receipts and a narrative clearly explaining the business purpose of the expenditure. Expense processors are required to bring disbursements that appear excessive or appear to be for non-business expenses to the attention of management. Expense reports submitted for less than $50 are required to be returned unprocessed with instructions to use petty cash. Also, Company policy requires VP approval for all expenses over $1,000. Approval authority for lesser amounts is tiered based on level in management.

Mr. Eversharp also recognizes that the process of coding and checking disbursements is susceptible to errors. For this reason, he placed his right hand man, Jack Johnson, in charge of quality control. Johnson personally reviews 50% of all disbursements on a weekly basis and verifies coding, approval, and business purpose. Since Johnson believes strongly in individual accountability, the results of his spot checks are incorporated into the Performance Management Process (PMP). PMP clearly outlines each employee's Major Responsibilities and Performance Standards. In his opinion, the existence of a standard company-wide coding manual means there should be no errors in his unit. He is frequently disappointed.

Mr. Eversharp also requires a detailed analysis of expenses by ledger code for each department. Significant variances from prior year or budget are discussed in weekly senior staff meetings, and department managers are required to submit action plans to get back on track. RLC's VP, Ms. Burleson, holds Mr. Eversharp personally responsible for variances by basing 100% of his bonus on meeting plan.

Key University of Toledo Policies

- Bylaws of the Board of Trustees
  (appointment/powers/authority, meetings, conflict of interest, etc.)
- Administration
  (finance/budgeting, legal affairs, IT, facilities, advancement, etc.)
- Human Resources
  (timekeeping, discipline, absence, standards of conduct, benefits, etc.)
- Academic
  (research, intellectual property, faculty, law, medicine, graduates, etc.)
- Main Campus Students
  (FERPA, grievances, financial aid, hazing, drugs, gambling, etc.)
- Athletics
  (recruiting, agents, game attendance, outside income, medicine, etc.)
- University of Toledo Medical Center
  (HIPAA, HITECH Law, Stark Law, Joint Commission, billing, etc.)

Should Internal Auditors Design Controls?

Internal auditors need control design skills when they:

- Participate in business process reengineering teams
- Perform internal consulting reviews
- Participate in systems development projects
- Are asked for advice about individual control issues
- Help management in any other way to build the right controls into a system on the front end, rather than waiting to catch the errors after they have occurred

In performing such reviews, we must remain independent, as defined by the *Standards for the Professional Practice of Internal Auditing*

- **1110 – Organizational Independence**
  The chief audit executive should report to a level within the organization that allows the internal audit activity to fulfill its responsibilities.
- **1120 – Individual Objectivity**
  Internal auditors should have an impartial, unbiased attitude and avoid conflicts of interest.
- **1130 – Impairments to Independence or Objectivity**
  If independence or objectivity is impaired in fact or appearance, the details of the impairment should be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

Even aside from the "proactive audit" activities listed on the previous page, internal auditors need control design skills during the course of normal audit activities. Audit situations requiring these skills include:

- Evaluating the adequacy of control system design.
- Recommending – or helping management develop – practical, cost-effective solutions to control problems identified during the audit.

UNIT SIX

SPECIAL CASES AND CHALLENGES

Overview

This unit deals with two topics of special interest to anyone who works with business controls. The first is fraud: what it is, why it occurs, and how to control it. The second is the Control Self-Assessment workshop technique for evaluating controls: what it is and why its use is growing rapidly today.

Objectives

Upon completion of this unit, you should:

- Have a basic understanding of the what, who, why, and how of fraud, as well as the role of business controls in preventing and detecting fraud.
- Understand why the Control Self-Assessment workshop technique is being used by a rapidly growing number of organizations, as well as how a workshop is conducted.

Fraud Quiz

1. Violent crimes cost the U.S.:

   A. $11 billion a year
   B. $98 billion a year
   C. $200 billion a year

2. White collar crimes cost the U.S.:

   A. $11 billion a year
   B. $98 billion a year
   C. $200 billion a year

3. Fraud is most likely to be perpetrated by:

   A. A recent hire who nobody knows very well
   B. A middle or senior level manager
   C. A front-line employee who handles cash regularly

4. Most common background for fraud perpetrators is:

   A. The military
   B. Finance and accounting
   C. Sales and marketing
   D. No background is more common than any other

5. An atmosphere of trust:

   A. Is an essential business control
   B. Openly invites fraud

Fraud Myths / Fraud Facts

Myth 1 – Normal people do not commit frauds

Fact: According to most fraud experts, in a typical organization:

10-20%	of employees would never commit a fraud, regardless of the situation	
60-80%	of employees could become perpetrators if the conditions were right	In other words, 80-90% are potentially perpetrators
10-20%	of employees are basically dishonest and will steal if they get a chance	

Ethics Quiz

Do you consider the following actions justified?	**Yes**	**No**
1. Taking money from the petty cash fund.	___	___
2. Taking a bribe from a superior.	___	___
3. Accepting a gift from a salesman.	___	___
4. Submitting the same expense item twice.	___	___
5. “Rounding up” the reimbursement for a $5.45 lunch.	___	___
6. Taking office supplies for your child at the start of school.	___	___
7. Making personal photocopies at work.	___	___
8. Using frequent flyer miles accumulated on company trips for a personal vacation should your company policy state that the miles belong to the company.	___	___
9. Coming to work late.	___	___
10. Not discussing a performance problem with an employee.	___	___
11. Exceeding the speed limit.	___	___
12. Saying you like your significant other’s cooking when you don’t.	___	___
13. Making personal long distance calls on your office phone.	___	___

What Would It Take To Make You Steal? (Profile of a Perpetrator)

Fraud experts agree that three things, in combination, tend to turn ordinary people into fraud perpetrators:

Pressure	Opportunity	Justification
• Financial crisis	• Weak control environment/ lax management	• "I'm just borrowing it; I'll pay it back"
• Gambling/drinking/ drugs (perpetrator or family member)	• Missing or weak control activities (especially segregation of duties)	• "My daughter is sick"
• Living beyond means	• Lack of monitoring	• "Everybody does it"
• Poor money management	• Lack of communication	• "They don't pay me enough"
• Affairs		• "I need it worse than the company"
• Mid-life crisis		• "It's for a good purpose"
• Feeling unappreciated • or underpaid at work		
• Greed		

Adapted from *Fraud – Bringing Light to the Dark Side of Business*, by W. Steve Albrecht, Gerald W. Wernz, and Timothy L. Williams, published by Irwin Professional Publishing, 1995

Fraud Myths / Fraud Facts

Myth 2 – It doesn't exist in our organization. If it does, it is not significant.

Fact:

KPMG Peat Marwick (1993) surveyed 2,000 of the largest companies in the U.S. in 1993. The survey results provided by 330 firms leave no doubt the fraud is a significant problem for business. More than 75% of the respondents experienced fraud during the previous year, with 23% reporting losses of $1 million or more. More than half of the respondents experienced up to 5 incidents of fraud. 25% observed more than 21 cases of fraud. The three **most expensive** types of fraud were **patent infringement**, **credit card fraud**, and **false financial statements**, each totaling more than $1 million per company involved. The **most frequent** type of fraud was **misappropriation of funds**, accounting for 20% of all fraud reported. This was followed by check forgery (19%), credit card fraud (15%), false invoices (15%), and theft (12%). Other types of fraud reported include accounts receivable manipulation, false financial statements, diversion of service, phantom vendors, purchases for personal use, diversion of sales, unnecessary purchases, vandalism, and sabotage.

Internal controls were cited most frequently as the reason frauds are discovered (59%). Review and specific investigation by management were the next two most frequently mentioned methods of discovery.

Poor internal controls were identified as the **most frequent reason** that **frauds occurred** (56% of respondents). Collusion between employees and third parties was an important factor in 44% of cases. Management overrides of existing controls occurred in 40% of the cases. Almost half (48%) of respondents indicated that there were "red flags" such as changes in employee's life styles or spending habits that pointed to the possibility of fraud, but they were ignored or not acted upon quickly enough.

Fraud Myths / Fraud Facts

Myth 3 – Preventing and detecting fraud is the internal auditor's responsibility

Myth 4 – Preventing and detecting fraud is management's responsibility, not the internal auditor's

Fact: Practice Advisories in the IIA Professional Practices Framework clarify Responsibilities related to fraud. The central point made by the Practice Advisories is:

- The principal deterrent to fraud is control (broadly understood), and management has primary responsibility for control.
- Internal auditing is responsible for evaluating control, commensurate with the potential risks.
- In evaluating control, internal auditing should determine whether
  - A strong control environment exists
  - Realistic goals and objectives are set
  - Written policies (e.g., code of conduct) describe prohibited activities and penalties for violations
  - Appropriate authorization policies exist
  - Appropriate policies, procedures, reports, and other mechanisms to monitor activities and safeguard assets exist
  - Communication channels provide management with reliable information
  - Recommendations should be made to improve cost-effective controls over fraud

Internal Auditor's Responsibilities
(Continued)

- The internal auditor's responsibilities for detection of fraud are to:
    - Have sufficient knowledge of fraud to be able to identify indicators
    - Be alert to opportunities, such as control weaknesses, which could allow fraud
    - If indicators of fraud are found, perform tests to identify further indicators
    - Evaluate the indicators and, if necessary, recommend an investigation
- Internal auditors are not expected to have knowledge equivalent to that of a person whose primary responsibility is detecting and investigating fraud. Also, audit procedures alone do not guarantee that fraud will be detected.
- If an investigation is performed, internal auditors may, within the limits of their knowledge, participate.

Some Common "Red Flags" Of Fraud

- Employee won't take a vacation
- Complaints about an employee
- Changes in employee lifestyle, habits, behavior
- Decline in employee morale and/or attendance
- Operating on a crisis basis
- Unexplained vacancies
- One employee "does it all" and wants to control everything
- Adversarial attitude towards control functions
- Inappropriate association with suppliers or inventories
- Missing or altered documents
- Invoice items do not appear consistent with the charge code and/or the business function
- Circumvention of the approval process (e.g., splitting purchases to keep each purchase below the threshold requiring approval)
- Excessive rush or emergency orders
- Vendors with generic names (XYZ, ABC)
- Vendors with only a post office box
- Transactions processed outside the normal channels (e.g., manual checks)
- Reconciliations not performed; failure to investigate reconciling items fully
- Even amounts on checks or documents
- Missing reports or documents
- Duplicate payments or documentation is not original
- Frequent use of management override (e.g., approval to process exception items)

Control Self-Assessment Workshops
- Overview –

Basic Methodology

Employees responsible for an activity evaluate the controls and identify opportunities for improvement during a 3-8 hour facilitated workshop.

Advantages

- Addresses “soft” environmental controls effectively
- Produces more and higher quality recommendations
- Leads to more timely implementation of recommendations
- Increases employee understanding and “ownership” of control
- Increases participant understanding of the business
- Allows more frequent and comprehensive coverage

Why we need to know about it:

- Major trend in business
- Based on the risk assessment thought process
- Self-assessment is an extension of the joint assessment performed in completing a risk/control matrix

Control Self-Assessment
- The Air Touch Communications Approach –

First Session (about 4 hours):

1. Introduce CSA and Train Participants

The introduction and training could take up to one and a half to two hours. The time necessary varies by the participants' concerns, enthusiasm and personal involvement.

To begin:

a) Provide a short information segment outlining the Control Self-Assessment process.
b) Discuss what to expect during the workshop.
c) Explain how the workshop fits into the overall process and the objectives of the CSA session.
d) Perform a brief training session tailored to participants' experience levels on objectives, risks, and controls.
e) Explain the risk ranking matrix and how it is used.

2. Facilitate Participants' Generation of Objectives, Processes and Risks

Generating ideas to describe objectives, processes and risks may take two to three hours. Design brainstorming exercises to stimulate participants' ideas, and to capture these thoughts using one of the quality tools.

To begin:

a) Brainstorm business objective for doing what they do. This task takes approximately 20 min.
b) Identify key processes relating to the subject. This task takes approximately 30 min.
c) Identify key risks associated with the key processes. This task takes approximately 20 min.
d) Select the top six key processes and associated risks. This task takes approximately 15 min.
e) Insert top six into the risk ranking matrix. This task takes approximately 5 min.
f) Rank the matrix. This task takes approximately 15 min.
g) Collect ranked matrix and tabulate between sessions.

CSA Workshop – Air-Touch Communications
(Continued)

Second Session (about 4 hours)

Select the process ranked as the highest risk area for a control breakdown and generate participant ideas on the following:

- Opportunities for improvements (Why a problem?)
- Suggestions for improvements (What needs to be done?)
- Action plans (How we are going to improve the process?)

After completing the first process assessment, select the process ranked the second highest risk area and perform the same process again. Continue this process until there is no more time available or as long as the participants would like to continue. It takes about 4 hours to generate action plans for three processes.

Explain to the participants what will be done with the information gathered during the session.

After the Session: Summarize & Report CSA Results

- Gather and summarize CSA information.
- Distribute the draft report to participants for review.
- Incorporate participants' comments into the report.
- Present local management with the CSA report.
- Obtain local management's comments and responses to the issues and action plans.
- Incorporate the CSA issues into the any Audit Reports with management's response.
- Attach summarized details to the audit report (optional).

Workshop Simulation
- Super Fliers –

General Background

Super Fliers was founded in 1980 and sells model planes and rockets. The company's headquarters and main equipment inventory warehouse is located in Chicago, Illinois. Plane & Rocket Kits, accessories, and repair parts are purchased directly from ten manufacturers. The warehouse services the six company-owned retail sales locations: Minneapolis, Pittsburgh, St. Louis, Omaha, Madison, and the store front adjacent to the warehouse in Chicago. The warehouse also provides inventory to sales representatives and two larger retail chains.

The aeronautical, remote control model business has experienced rapid growth during the last few years. The growth is primarily due to the dramatic decrease in the cost of electronic technology, which makes it more affordable for the average consumer to support this hobby. In addition, Super Fliers has had several sales promotions during the year, making aeronautical models even more appealing. The company is planning to open three new retail sales locations by year-end. They also plan to launch creative new promotions during the holiday season. This is expected to result in huge increases in sales volumes.

The following prior year information is available for the company.

- Sales were valued at $12,000,000 at year end
- Accounts receivable was valued at $3,000,000 at year end.
- Over 10,000 inventory items are processed monthly.
- Each retail sales location and distributor places inventory orders at a minimum of twice weekly.
- Due to invoicing constraints and multiple shipments on one invoice, approximately 3,000 sales transactions are processed per month.

Due to the dramatic growth, Super Fliers is thinking about purchasing a new point-of-sales, inventory and sales management system in the next year. The current system does not provide an automatic interface to the general ledger. It does, however, have the functionality necessary to scan in and out inventory items from the system. The system crashes about once a month. When this occurs it takes anywhere from 6 to 24 hours to resolve the system problems. If the system goes down during special product promotions, stock may be difficult to access in a timely manner. During the last promotion, order processing had a five day backlog of data entry resulting from a system crash.

Special Cases and Challenges

The last physical inventory count and reconciliation to the accounting records took place late last year (about nine months ago), no physical counts have yet been performed this year.

The inventory warehouse has nine employees: an inventory manager, five warehouse clerks, two receiving/shipping clerks, and an equipment repair person. These employees work within the warehouse, and their desks and office space are also within the perimeter of the warehouse. The company accounting manager and accounts payable person visit the warehouse frequently to obtain information and documentation for processing inventory data. Since the warehouse is located next to a store front, sales representatives and other employees are regularly visiting the inventory location to deliver or pick up orders.

The CSA team has been to Super Fliers' Chicago location to conduct preliminary survey interviews related to inventory processes. They met with the General Manager, The Finance Director, the Accounting Manager and the Inventory Manager, have performed walkthroughs of the inventory processes, and obtained process flowcharts. Super Fliers management is committed to quality and sees CSA as a method to integrate quality concepts. Management feels that they have good controls over inventory management; however' they believe that they need a new inventory computer system to support their continued growth.

The CSA team has selected the following individuals to participate in the control Self-Assessment Workshops:

- Bob, Inventory Manager
- Jeff, Accounting Manager
- Sam, Shipping/Receiving Clerk
- Shirley, Warehouse Clerk
- Joe, Warehouse Clerk
- Esmeralda, Accounts Payable Clerk

Special Cases and Challenges

Group Activity

- Break into small teams.
- Choose one of your department's business processes to self-assess.
- Identify 3-5 key business objectives for the process you selected.
- Choose **one** of the above objectives, and identify 3-5 risks to achieving that objective.
- Choose **one** of the above risks, and identify 3-5 controls that might address the risk.
- Record your observations using a table with the following headings:

Business Process Selected:		
Objective	**Risks**	**Controls**

- Remember the one-to-many relationship between business objectives, risks, and controls.
- Choose a volunteer to present your findings.
- Present.
- 15 minutes within your teams.

THE UNIVERSITY OF TOLEDO 1872

Summary

THE UNIVERSITY OF TOLEDO 1872

THE UNIVERSITY OF TOLEDO 1872

Overheads

"Internal Controls and You" (risk assessment and risk management training)

Presented by:
The University of Toledo Internal Audit Department
David L. Cutri, Chief Audit Executive
530-8718

Overview

This course covers the essential terminology of risk and control. It also provides an overview of commonly used risk and control frameworks. In addition, examples of how to critically evaluate risks for your organization are provided.

Objectives

By the end of this course, you should be able to:

- Identify the components of risk assessment and risk management as they relate to internal controls.
- Establish a risk management and internal controls strategy for your business unit
- Identify and be able to apply key University policies and procedures.

Overheads

What Is Business Risk Management?

- "A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives" (The Institute of Internal Auditors)
- In other words, business risk management is the identification of key **business objectives** within a process, **risks** to achieving these business objectives, and the internal **controls** in place to resolve the risks identified.

Who Is Responsible for Business Risk Management?

YOU !!!

(the process owner)

What Are Business Objectives?

- **"**Goals or targets that a business sets for itself, they differ according to the type of business." (Wiki Answers)
- In other words, business objectives summarize **the work you accomplish every day**.

Overheads

Sources for Identifying Business Objectives

- "Charge" for Your Business Function
  - "Charges" for high-level functional areas such as academic and student affairs, clinical affairs, external affairs, finance, trusteeship and governance, strategic planning, and audit are approved by the Board of Trustees
- Operating Plan for Your Department
- Your Department's Intranet Site
- Your Performance Evaluation
- External guidance is also available for you to identify your business objectives, in the form of methodologies such as "COSO", "CobIT", and "CoCo"

COSO Methodology

- COSO (Committee Of Sponsoring Organizations) was developed in 1992 by The Treadway Commission.
- COSO states that all business objectives can be categorized/"bucketed" as follows:
  - Effectiveness and efficiency of operations
  - Reliability of financial reporting
  - Compliance with applicable laws, regulations, and guidelines
- More on COSO later in the course …

What Are Key Business Risks?

- "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." (The Institute of Internal Auditors)
- In other words, business risks are **the barriers or impediments to successfully achieving the business objectives** established by the process owner.
- Typically, a single business objective will have several business risks associated with it.

Overheads

Risk Assessment Concepts and Terms

Following are risk assessment terms and concepts:

- Inherent risk
- Residual risk
- Risk categories
- Risk events
- Impact
- Likelihood
- Speed of onset
- Materiality

What Are (Internal) Controls?

- "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." (The Institute of Internal Auditors)
- In other words, internal controls are the policies, procedures, and **business practices in place to reduce the likelihood that identified risks will occur**.

What Are Internal Controls (Continued)?

- Internal controls provide reasonable, but not absolute, assurance that business risks will not be realized. Absolute assurance is very difficult, and often not cost-effective, to achieve.
- Typically, a single business objective will have several business risks associated with it, and a single business risk will have several internal controls associated with it.

Overheads

COSO Internal Control Framework

- The COSO framework discussed previously states that all internal controls can be categorized/"bucketed" as follows:
  - Control Environment ("tone at the top")
  - Risk Assessment
  - Control Activities (policies, procedures, business practices)
  - Information and Communication
  - Monitoring

A pictorial representation of the COSO framework is documented in the COSO cube to the right.

Control Concepts and Terms

Control concepts and terms:

- Preventive control
- Detective control
- Manual control
- Automated control
- Hard control
- Soft control
- Key control

"Driving to Work"

Some key business **objectives** …

- Safely get to work
- Quickly get to work
- Efficiently use a route that saves on gas
- Thoughtfully minimize disruption to coworkers through carpooling
- Carefully drive so as to avoid getting a ticket

Overheads

"Driving to Work" (Continued)

Some **risks** to the objective of getting to work safely …

- Accidents
- Inattentive fellow drivers
- Obstacles in the road
- Unclear road signs
- Construction

"Driving to Work" (Continued)

Some **controls** pertinent to the objective of getting to work safely, and the risk of accidents …

- Wake up two hours before work starts
- Check driver's forecast on TV
- Maintain a three-car distance from car in front of you
- Adhere to maintenance schedule from your car's owner's manual
- Refer to MapQuest in identifying a route without construction and follow it

"Paying the Bills – Accounts Payable"

Some key business **objectives** …

- Accurately and completely making and recording cash disbursements on a timely basis.
- Minimizing processing time
- Properly authorizing accounts payable and cash disbursements.
- Developing strategic business alliances with suppliers
- Using reliable performance measurements to control and improve the process.

Overheads

"Paying the Bills – Accounts Payable" (Continued)

Some **risks** to the objective of accurately and completely making and recording cash disbursements on a timely basis …

- Inaccurate transaction coding and posting errors in the accounts payable trial balance may result in non-value-added activity to correct the errors.
- Not recording purchases and cash disbursements on a timely basis
- Making payments to the wrong parties and recording disbursements for the wrong amounts because of clerical or mechanical processing errors.
- Credit and debit memos may be missing from the records because of errors like unrecorded adjustments.
- Purchase discounts may not be accurately calculated and properly recorded.

"Paying the Bills – Accounts Payable" (Continued)

Some **controls** pertinent to the objective of accurately and completely making and recording cash disbursements on a timely basis, and the risk of incorrect coding and posting …

- Use batch totals before completing the payment process for computer systems that input disbursements into a temporary file.
- Check quantities, prices, extensions and footings of invoices, accuracy of account distribution, and proper approvals prior to general ledger journal entry.
- Establish procedures to ensure period end reconciliation of the accounts payable ledger to the general ledger as well as to correct cut-off errors on a timely basis.
- Review unprocessed receiving reports and invoices periodically, and investigate and resolve them.
- Determine control totals prior to inputting invoices. Ensure computer routines reconcile this amount to the total of invoices accepted or rejected during systems processing.

Evaluating Controls

- It is not enough to identify controls that might address known risks.
- You should also be creative and identify what controls you would expect to be in place.
- Compare these expected controls to the actual controls in place and identify gaps (residual risk).
- You will then need to make a determination as to whether these residual risks should be addressed. Consider such factors as cost, compliance with regulations and policy, etc.

Overheads

Evaluating Controls (Continued)

- You may not be in a position (organizationally) to address residual risks.
- As a result, you may have to formulate a recommendation for corrective action.
- Modifying the risk matrix in the following way (below) may be helpful in establishing your business case …

Business Process:						
Objective	Risks	Expected Controls	Actual Controls	Residual Risk	Recommendations	Action Plan
Several per business process	Several per objective	Several per risk				

Control Testing

- As a process owner, you should have a way of satisfying yourself that the controls you believe are in place are functioning as you intended them.
- As such, you should establish a schedule for regularly testing key controls. Test plans should be developed and documented, and should include the following …
  - Business process
  - Business sub-process
  - Modules (if applicable)
  - Objective of test
  - Test plan (narrative)
  - Error conditions tested
  - Expected results
  - Actual results
  - Link to test data
  - Test conclusion
  - Next steps (if applicable)
  - Name of tester
  - Date of test
- Internal Audit and other departments can be helpful in helping you establishing a control testing program.

Who Is Responsible for Business Risk Management?

- **YOU !!!** (the process owner)
- But you are not alone.
- Several other resources are available to help you manage risk, including …
  - Internal Audit
  - Compliance
  - Controller's Office
  - Business Managers
  - Legal Affairs
  - Human Resources
  - Your Supervisor
  - Local Compliance Officers
  - Policies Website
  - External Auditors (Plante and Moran)
  - Anonymous Reporting Line
  - Joint Commission
  - Auditing Institutes (National and State)
  - Vendor Literature

Overheads

A Word about the Internal Audit Department

- **Our Charge:** "… oversight and continuous improvement of fiscal and other controls for the University and insures that the fiduciary responsibility of the Board is carried out." "…insure that the highest ethical and legal standards are met."
- In other words, independently and objectively evaluate the effectiveness of the risk management activities of the process owner.
- "Lines of Business"
  - ➢Financial and operational audits
  - ➢Information Technology audits
  - ➢Compliance reviews
  - ➢Control Self-Assessments
  - ➢Business Process Improvement
  - ➢Commercial contract reviews
  - ➢Best practice reviews
  - ➢Ethics investigations
  - ➢Data privacy audits
  - ➢Continuous controls monitoring

Key University of Toledo Policies

- Bylaws of the Board of Trustees
  (appointment/powers/authority, meetings, conflict of interest, etc.)
- Administration
  (finance/budgeting, legal affairs, IT, facilities, advancement, etc.)
- Human Resources
  (timekeeping, discipline, absence, standards of conduct, benefits, etc.)
- Academic
  (research, intellectual property, faculty, law, medicine, graduates, etc.)
- Main Campus Students
  (FERPA, grievances, financial aid, hazing, drugs, gambling, etc.)
- Athletics
  (recruiting, agents, game attendance, outside income, medicine, etc.)
- UT Medical Center
  (HIPAA, HITECH Law, Stark Law, Joint Commission, billing, etc.)

Group Activity

- Break into small teams.
- Choose one of your department's business processes to self-assess.
- Identify 3-5 key business objectives for the process you selected.
- Choose **one** of the above objectives, and identify 3-5 risks to achieving that objective.
- Choose **one** of the above risks, and identify 3-5 controls that might address the risk.
- Record your observations using a table with the following headings:

Business Process Selected:		
Objective	**Risks**	**Controls**

- Remember the one-to-many relationship between business objectives, risks, and controls.
- Choose a volunteer to present your findings.
- Present.
- 15 minutes within your teams.

Overheads

Summary

Notes

Notes

Notes

Notes

Notes

Notes

Notes

Notes

Notes

Notes