April 6, 2011

# Best Practices for Using Internal Controls to Meet Financial and Operational Objectives

Joe Belcher, University Coordinator of Business Practices

VirginiaTech
Invent the Future

# Course Objectives

- Describe VT’s Paradigm of Control
- Understand, identify, and assess risks
- Understand internal control, what can override it, and its basic principles
- Better mitigate risks impacting your department so financial and operational objectives may be met
- Understand the importance of monitoring internal controls

VirginiaTech
Invent the Future

# VT's Paradigm of Control

## The Old Way

Encounter Problem

↓

React to Problem

↓

Install Control to Fix Problem

↓

Manage the Patched Structure

## The New Way

Understand Key Business Objectives

↓

Identify Problems (risks)

↓

Strengthen / Eliminate Controls

↓

Monitor Effectiveness of Controls

VirginiaTech
Invent the Future

# What is Risk?

Risk is the threat that an event or action will adversely affect an organization’s ability to achieve its objectives and/or execute its strategies successfully

***"Every time we see a big crisis, someone messed up the risk management."***

CNN article on Bear Stearns – March 17, 2008

# Types of Risk:

- Strategic risks – doing the wrong things
- Operating risks – doing the right things the wrong way
- Reporting risks – not having accurate and/or complete information
- Compliance risks – not following laws, regulations, policies or procedures

# Types of Risk:

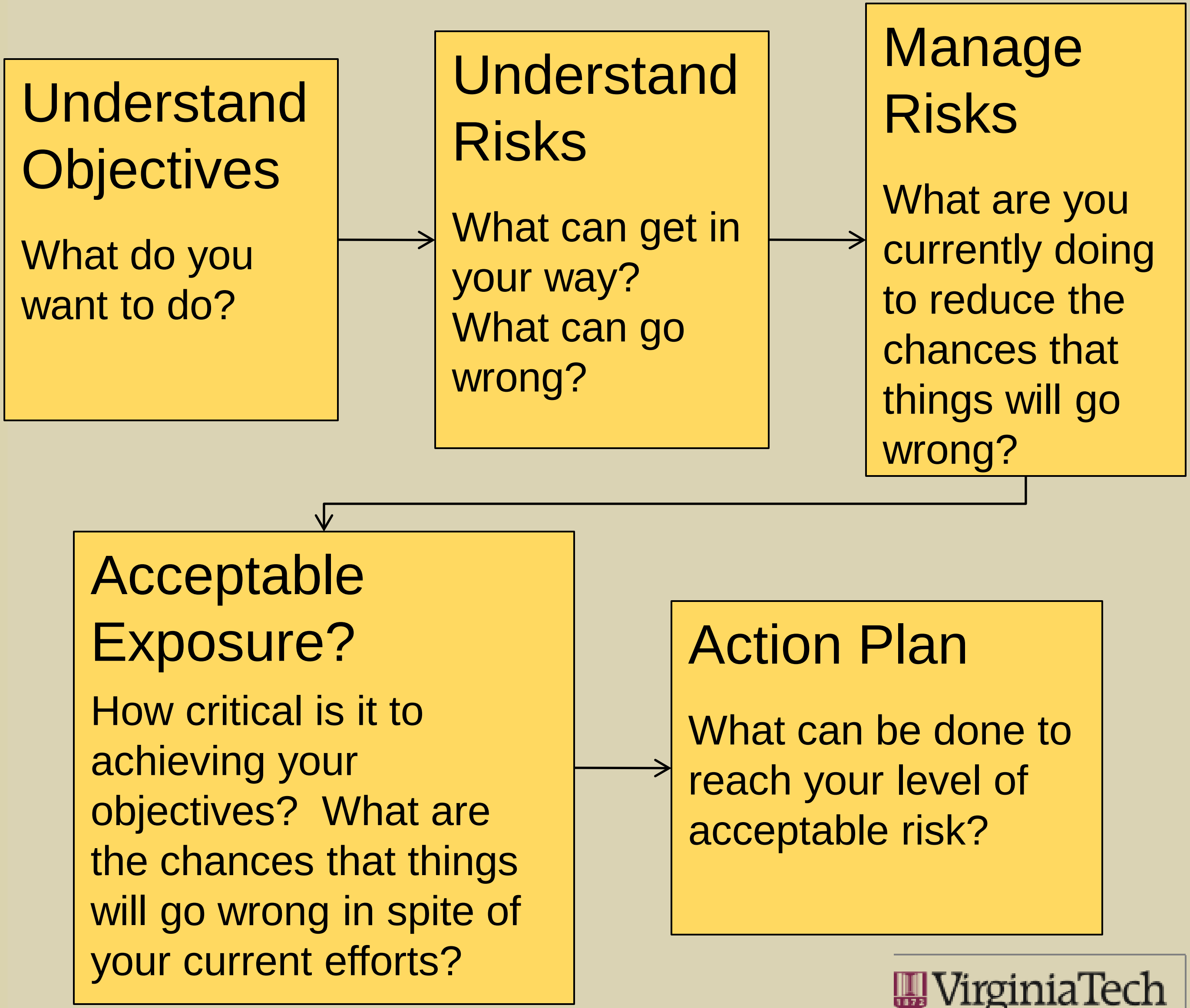
- Financial risks – losing financial resources or incurring unacceptable liabilities
- Information risks – inaccurate or non-relevant information, unreliable systems, and inaccurate or misleading reports
- Physical risks – loss of computer data, fire, catastrophe, injury to people
- Human capital risks – worker safety, employee travel, workplace violence

VirginiaTech
Invent the Future

# Types of Risk:

- Legal risks – employment practices, general / premise liability
- Environmental risks – degradation of the environment
- Political risks – local, state, national and international pressures
- Technological risks – Computer viruses new technologies, hackers, technology implementation failure

# Framework for the Management of Risks



**Understand Objectives**

What do you want to do?

**Understand Risks**

What can get in your way?
What can go wrong?

**Manage Risks**

What are you currently doing to reduce the chances that things will go wrong?

**Acceptable Exposure?**

How critical is it to achieving your objectives? What are the chances that things will go wrong in spite of your current efforts?

**Action Plan**

What can be done to reach your level of acceptable risk?

# Risk Management Techniques:

1. Accept: Do nothing
2. Eliminate: Stop doing the activity
3. Transfer: Got Insurance?
4. Reduce (mitigate): Internal Controls!

VirginiaTech
Invent the Future

# What are Internal Controls?

Internal Control is a **process** designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

➢Effectiveness and efficiency of operations

➢Reliable financial information

➢Compliance with applicable laws and regulations

# Internal Control Process

Internal Control consists of five interrelated components:

- **Control Environment (Tone at the Top)**
- **Risk Assessment**
- **Control Activities**
- **Information and Communication**
- **Monitoring**

VirginiaTech
*Invent the Future*

# ICP - Control Environment

Defined as the control consciousness of an organization. Leaders should foster a control environment that encourages:

➢The highest level of integrity and professional standards

➢The promotion of internal control throughout the organization

➢Assignment of authority & responsibility

*Tip: The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable.*

# Control Environment Tips:

- **Departmental policies & procedures** are documented. Specific activities and unique issues have been addressed.
- **Employee responsibilities** are documented and understood: limits to authority, control procedures, performance standards, and etc.
- **University's policies & procedures** are understood by employees; especially those policies specifically related to their jobs.
- **Adequate training** is available for employees.
- **Clearly defined job descriptions** exist and include the specific responsibilities associated with internal controls.

VirginiaTech
Invent the Future

# ICP - Risk Assessment

The central theme of internal control is:

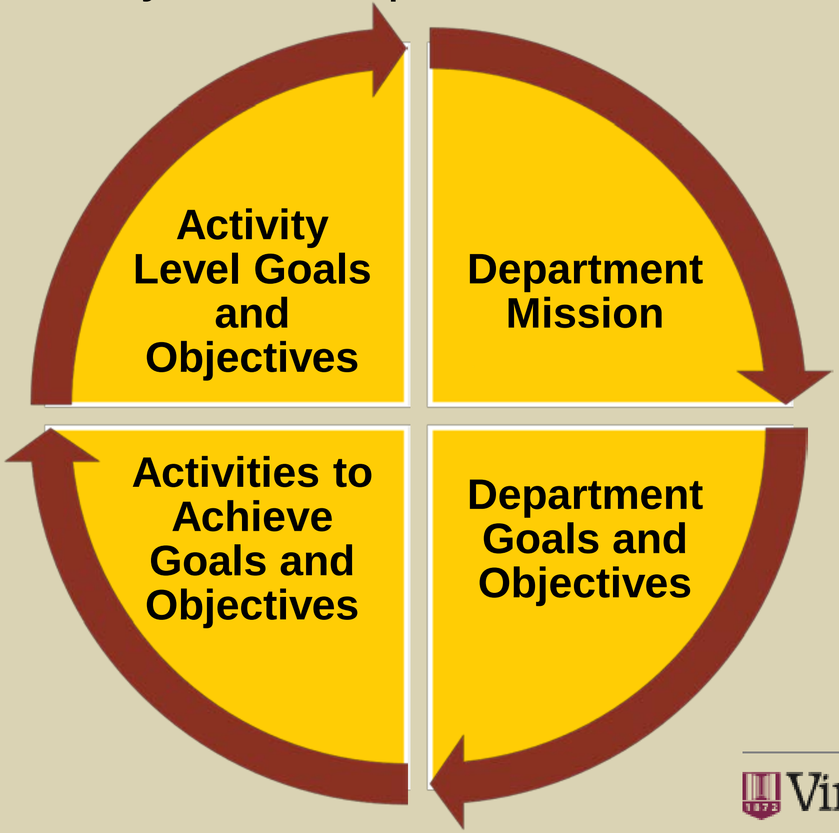
1. **to identify risks to the achievement of an organization’s objectives and**
2. **to do what is necessary to manage those risks**

Therefore, actually setting goals & objectives is a precondition to internal control.  Goals & Objectives are classified in the following way:

- **Operational objectives – achieving the basic mission(s) of a department and the effectiveness and efficiency of its operations**
- **Financial reporting objectives – preparation of reliable financial reports**
- **Compliance objectives – adherence to applicable laws and regulations**

# Risk Assessment

A clear set of goals & objectives is a key to success. A department or unit should have (1) a mission statement, (2) written goals & objectives for the department as a whole, and (3) written goals & objectives for each significant activity in the department.



Department Mission

Department Goals and Objectives

Activities to Achieve Goals and Objectives

Activity Level Goals and Objectives

VirginiaTech
Invent the Future

# Identify risks after determining goals

Risk assessment: identification & analysis of risks associated with the achievement of objectives

- ➢What decisions require the most judgment?
- ➢How could we fail?
- ➢What must go right for us to succeed?
- ➢Where are we vulnerable?
- ➢What assets do we need to protect?
- ➢How could someone steal from the department?
- ➢How could someone disrupt our operations?
- ➢How do we know whether we are achieving our goals?
- ➢How could we go wrong?

VirginiaTech
Invent the Future

# Risk Identification Example:

## HokieMart Process Objectives

1. **Purchases comply with federal, state, and university procurement policies, laws, and regulations**
2. **Fraud and misuse are kept to a minimum**
3. **Approved goods and services, as specified by the users of the goods and services, are received promptly**
4. **Costs for goods and services are reasonable and appropriate**
5. **Payment for goods and services received is made on a timely basis**
6. **All transactions are accurately recorded to allow for the preparation of meaningful internal and external reports**
7. **Sufficient documentation for each transaction is retained as evidence of the expenditure's appropriateness**

VirginiaTech
*Invent the Future*

# Risk Identification Example:

## HokieMart Process Objectives

| Process Objective | Risks/***Consequences*** |
|---|---|
| Purchases comply with federal, state, and university procurement policies, laws and regulations | Purchases might not be in compliance with federal, state, and/or university procurement policies, laws and regulations<br>***Expenditures will be disallowed during an audit. Findings may provoke a unit or campus-wide audit*** |

VirginiaTech
*Invent the Future*

# Risk Identification Example:

## HokieMart Process Objectives

| Process Objective | Risks/***Consequences*** |
|---|---|
| Fraud and misuse are kept to a minimum | Payments could be made for goods and services never received or intended for the university's use<br>***Resources will not be available for legitimate expenditures*** |

VirginiaTech
Invent the Future

# Risk Identification Example:
## HokieMart Process Objectives

| Process Objective | Risks/***Consequences*** |
|---|---|
| Approved goods and services, as specified by the users of the goods and services, are received promptly | Goods and services might be ordered without proper approval being given<br>***Goods or services might not actually be needed resulting in reduced funding for future needs*** |

VirginiaTech
*Invent the Future*

# Risk Identification Example:

## HokieMart Process Objectives

| Process Objective | Risks/***Consequences*** |
|---|---|
| Approved goods and services, as specified by the users of the goods and services, are received promptly | •The goods & services received might not be the quantity, standard, or type of goods specified by the user<br>•There could be an inordinate amount of time between when the users express the need for goods and services, and the receipt of those goods and services<br>***The goods and services might not be useful to the research, resulting in staff time required to return goods and/or reduced funding for future research*** |

VirginiaTech
Invent the Future

# Assessing a Risk's Impact

**Consider both qualitative and quantitative costs:**

***Quantitative*** Costs Include:

- Cost of property, equipment, or inventory
- Cash dollar loss
- Damage and repair costs
- Cost of defending a lawsuit

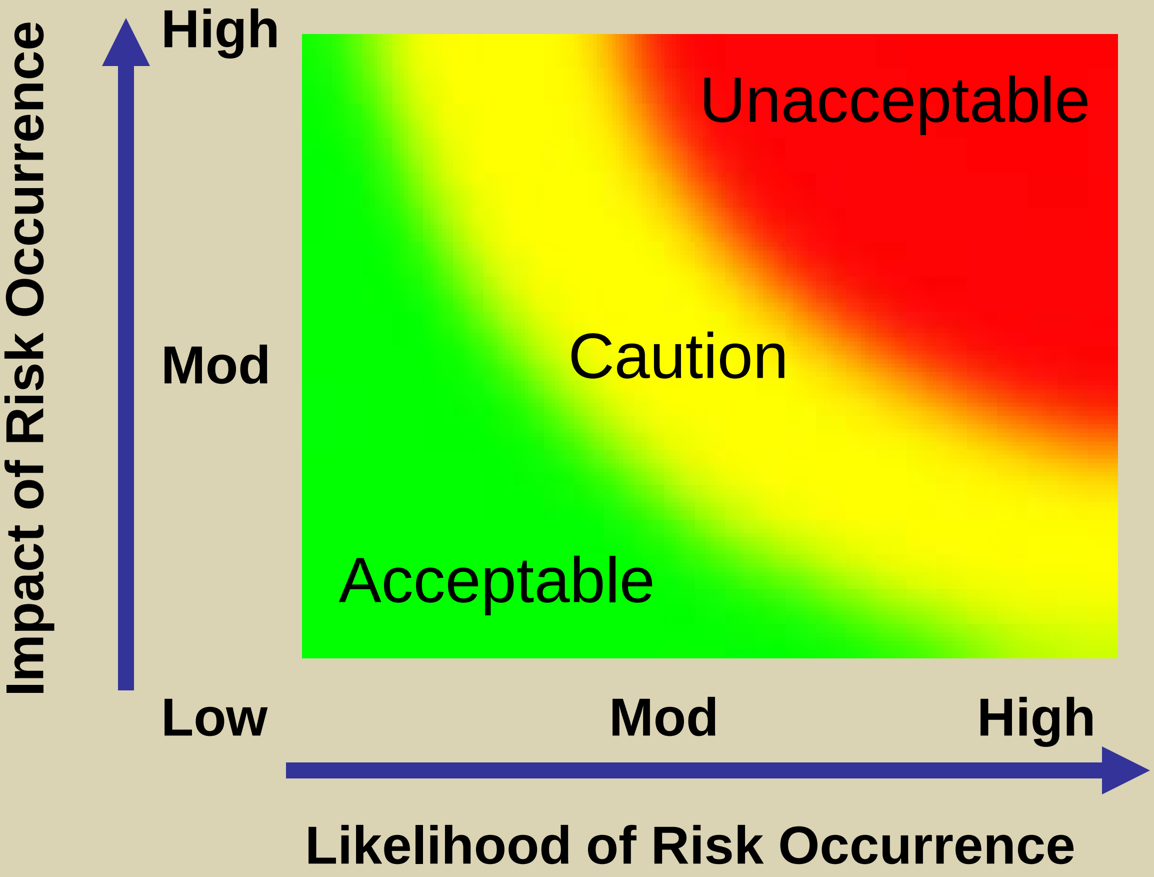
***Qualitative*** Costs Include:

- Loss of future grants, gifts, and donations
- Increased legislation
- Loss of public trust
- Injury to the Unit's and/or the University's reputation
- Bad publicity

VirginiaTech
Invent the Future

# Combinations of frequency and significance expose the campus to various degrees of risk.

**Risk: *f*(Frequency x Significance)**



Impact of Risk Occurrence

High

Mod

Low

Unacceptable

Caution

Acceptable

Mod

High

Likelihood of Risk Occurrence

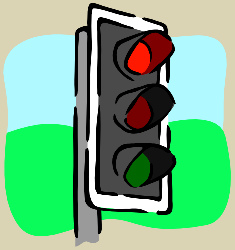
VirginiaTech
Invent the Future

# ICP - Control Activities

Defined as actions, supported by policies and procedures that, when carried out properly and in a timely manner, manage or reduce risks

## Categories of Control Activities:

- **Preventive** – Activities which can stop or preempt a potential problem or loss from occurring



- **Detective** – Controls which identify a potential problem or loss that has occurred

VirginiaTech
Invent the Future

# Control Activities – Key Points:

✓ People at every level of an organization affect internal control

✓ Internal control can provide only reasonable assurance (**not** absolute assurance) regarding the achievement of an organization’s objectives

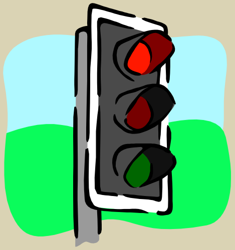
✓ The cost of a control should not exceed the benefit to be derived from it:

| Excessive Risks | Excessive Controls |
|---|---|
| Public Scandals | Reduced Productivity |
| Poor Business Decisions | Increased Complexity |
| Loss of Assets, Donors, or Grants | Increased Bureaucracy |

VirginiaTech
Invent the Future

# ICP - Control Activities

## Approvals (*Preventive*):



- ➢Limits to authority
- ➢Written policies and procedures
- ➢Supporting documentation
- ➢Question unusual items
- ➢No “rubber stamps”
- ➢No blank signed forms

❖Approvers should never allow someone else to sign for them

❖ An approver should never share his or her password with another person

VirginiaTech
Invent the Future

# ICP - Control Activities

## Reconciliations (*Detective*):

Comparing different sets of data to one another, identifying and investigating differences, AND taking corrective action

## Reviews (*Detective*):

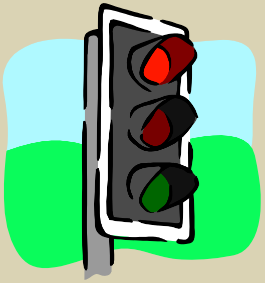
- **Budget to actual comparison**
- **Current to prior period comparison**
- **Performance indicators**
- **Follow-up on unexpected results or unusual items**

VirginiaTech
Invent the Future

# ICP - Control Activities

## Asset Security (*Preventive & Detective*):

- Security of physical & intellectual assets
- Physical safeguards
- Perpetual records are maintained
- Periodic counts / physical inventories
- Compare counts to perpetual records
- Investigate and correct differences

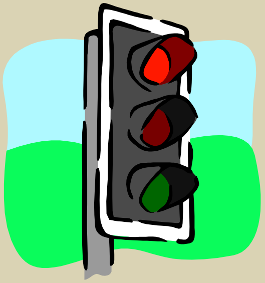


VirginiaTech
Invent the Future

# ICP - Control Activities

## Segregation of Duties (*prevent & detect*)

No one person should:



- Initiate the transaction
- Approve the transaction
- Record the transaction
- Reconcile balances
- Handle assets
- Review reports

At least two sets of eyes

VirginiaTech
Invent the Future

# ICP - Control Activities

**Information Systems – mainframe computers, single-user workstations, LANs & WANs, and etc.**

**The need for internal controls over these systems depends on the criticality and confidentiality of the information and the complexity of the applications present.  The two basic categories of controls are:**

- **General Controls – apply to entire information system and to all applications present**
- **Application Controls – apply to the computer programs and processes, including manual processes, that enable us to conduct essential activities: buying products, paying people, accounting for research costs, and etc**

VirginiaTech
Invent the Future

# Control Activities: Information Systems

**General controls consist of practices designed to maintain the integrity and availability of information processing functions, networks, and associated application systems.  General controls include:**

- **Access Security, Data & Program Security, Physical Security**
- **Software Development & Program Change Controls**
- **Data Center Operations**
- **Disaster Recovery**

# Control Activities: Information Systems

**Application controls consist of the mechanisms in place over each separate computer system that ensure that data is completely and accurately processed. Application controls include:**

- **Input Controls (data entry)**
  - **Authorization**
  - **Validation**
  - **Error Notification**
- **Processing Controls (record counts)**
- **Output Controls (error listings)**

VirginiaTech
Invent the Future

# ICP – Information & Communication

**Information and communication are essential to effecting control. The following information must be communicated up, down, and across an organization:**

- **Organization’s plans**
- **Control environment**
- **Risks**
- **Control activities**
- **Performance**

# ICP – Information & Communication

**When assessing controls over a significant activity, the key I & C questions to ask are:**

- Does our department get the information it needs in a form and timeframe that is useful?
- Does our department get information that alerts it to internal and external risks?
- Does our department get information that measures its performance – information that tells the department whether it is achieving its objectives?
- Does our department identify, capture, process, and communicate the information that others need in a form and timeframe that is useful?
- Does our department provide information to others that alerts them to internal or external risks?
- Does our department communicate effectively--internally and externally?

VirginiaTech
Invent the Future

# ICP – Monitoring

**Monitoring is the assessment of internal control performance over time; it is accomplished by ongoing monitoring activities and by separate evaluations of internal control such as:**

- **Self-assessments**
- **Peer reviews**
- **Spot checks**
- **Internal audits or compliance audits**
- **ARMICS Reviews**

VirginiaTech
*Invent the Future*

# ICP – Monitoring

**The purpose of monitoring is to determine whether internal control is adequately designed, properly executed, and effective. Internal control is effective if management has reasonable assurance that:**

- ✓ **They understand the extent to which operational objectives are being achieved**
- ✓**Published financial statements are being prepared reliably**
- ✓**The unit is in compliance with applicable laws & regulations**

VirginiaTech
Invent the Future

# Conclusion

Internal control is adequately designed and executed if all five of the internal control components (shown below) are present and functioning as designed

- ✓**Control Environment**
- ✓**Risk Assessment**
- ✓**Control Activities**
- ✓**Information and Communication**
- ✓**Monitoring**

While internal control is a process, its effectiveness is an assessment of the condition of the process at one or more points in time

# Questions?

???

VirginiaTech
Invent the Future