Strengthening Business Practices: The Language of Our Control Environment

University of California
Business Officer Institute

Control Environment Agenda

• Speaking a Common Language
  – What is Internal Control?
• The Right Controls at the Right Place?
  – A Five-Part Model
• Interactive Self Assessment
  – Attitudes Toward Risk and Control
• Resources
  – Role of the Controller, Auditor
We are *Like* a Business

- Good control is good business
- Good control is Everyone’s business
- Business Officers play an especially important role in our control systems

New Audit Requirements

- Statement of Auditing Standards (SAS) No. 112: *Communicating Internal Control Related Matters Identified in an Audit*
- Significantly tightens the requirements for public reporting of internal control deficiencies
...by the way, what is *Internal Control*?

A *process*, put in place by people, that is designed to provide *reasonable assurance* that we will achieve the following *objectives*:

1. Effectiveness and efficiency of operations
2. Reliability of financial reporting
3. Compliance with laws and regulations

**A Framework for Achieving Objectives**

Reference Document: *Understanding Internal Controls*
Management Environment

People and the Work Environment

The foundation of sound internal control
- Control Consciousness
- Tone at the top
- Ethics
- Integrity
- Accountability

Wouldn’t you agree?

Good people can make a bad system work, while bad people can make the best system fail
Risk Assessment

Identify, Analyze and Manage Risks

Understand Objectives → Understand Risks → Manage Risks → Acceptable Exposure

What are you trying to accomplish? → What gets in your way? → What are you doing to manage this? → Where do you feel exposed?

Control Activities

Business Policies and Practices

• Two types of control activity
  – Preventive
  – Detective

• Common control activities:
  – authorization, approval, reconciliation, review, asset security, separation of duties, information system controls
Monitoring

Analysis of Control Systems over Time

• Are our control practices keeping pace?
  – Ongoing monitoring activities
  – Separate evaluations

Good monitoring allows us to weather the storms of constant change
Information and Communication

Capture and Exchange of Key Data

• Getting the right information to the right people in time to make quality decisions

• Systems can be formal or informal
  – Formal: sophisticated computer systems
  – Informal: periodic staff meetings

Interactive Self Assessment

Attitudes Toward Risk and Control

• How do you view risk and control?
  – Personal perspectives affect the quality of our Control Environment

• Meet Mary, John and Bob
  – Your imaginary co-workers
Examples of Attitudes Toward Risk and Control

Mary, John and Bob all manage their personal money using checking accounts. One objective they have in common is to prevent unauthorized withdrawals from their checking accounts.

In the following scenarios, you will see statements that describe how Mary, John and Bob achieve this objective.

Scenario 1: Attitudes Toward Risk and Control

Objective: To prevent unauthorized withdrawals from their checking accounts

Control: Use a transaction register that includes all deposits, withdrawals, other charges and ending balances

I do not maintain a register. I rely on bank statements to be accurate.

Sometimes I update my register; I like to have it updated but sometimes I don’t do it.

I always update my register. One can never be too careful with money.
Scenario 2: Attitudes Toward Risk and Control

Objective: To prevent unauthorized withdrawals from their checking accounts

Control: Restricting withdrawal authority to the minimum number of people possible

Mary = high risk tolerance
John = medium risk tolerance
Bob = low risk tolerance

I am so busy with work and my personal time that sometimes my cousin stops by the bank for me. I trust my family; therefore I have 5 people authorized to make withdrawals.

On my account, my wife and I are authorized. We're pretty good about telling each other what withdrawals we make.

I only have myself authorized to make withdrawals. That way, if anything looks funny I will know right away that it is an error.

Scenario 3: Attitudes Toward Risk and Control

Objective: To prevent unauthorized withdrawals from their checking accounts

Control: Bank cash machines are programmed to keep the bank card after 4 failed password attempts to prevent someone from guessing the password

Mary = high risk tolerance
John = medium risk tolerance
Bob = low risk tolerance

There shouldn’t be any restrictions. When I am busy, sometimes I forget my password, then I have to get a new card. This is not a user friendly bank!

My password is hard to remember. It is so hard, that sometimes I have to enter it several times. Allowing 5 or 6 attempts is acceptable to me.

I think the rule should be 3 strikes and you’re out. I don’t want someone to have easy access to my cash at the ATM.
Bridging Between Home and Work  
*Comparative Differences*

How do my personal attitudes about risk and control differ between home and work?

1. Attitudes at work are more conservative than home
2. Attitudes at work and home are about the same
3. Attitudes at work are more liberal than home

Opportunities for Improvement  
*Where do I feel vulnerable?*

In my workplace, which area could use the most improvement to strengthen business practices?

1. Budgeting (process, not amount)
2. Handling cash
3. Purchasing / making payments
4. Information technology
5. Staffing / Human Resources
6. Not sure
Resources
Who can I call for help?

Controller
Line management champion of internal control

Auditor
Control consulting, evaluation of controls established by management

Colleagues
Everyone is responsible for internal controls

For Reference: Controllers and Auditors: Responsibilities within the Context of Internal Control

A Balancing Act

• Controls should be proactive, value-added and cost effective

• Cost of a control should not exceed the benefit derived from it