IT Governance & the Control Environment
Week 2
ISACA’s View of Governance

• What is IT governance? Define each of the components?

• How does this compare with the definition we used last week?

• Value Delivery
• Risk Management
• IT Strategic Alignment
• Resource Management
• Performance Management

• Doing the right thing
  – Value Delivery
  – Risk Management
• Doing it right
  – Strategic Alignment
  – Resource Management
  – Performance Management
What Does a Company Want From its IT Systems?

- Take 5 minutes and write down all of the attributes of an IT system that a company would want.
- For example: A company wants its IT systems to be available.
- Effective
- Efficient
- Confidential
- Integrity
- Available
- Compliant
- Reliable
What are controls? Controls are defined as the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented.
What types of controls are there?

- Preventive Controls
- Detective Controls
- Corrective Controls

Give me some examples?
What is the difference between general and application controls?

General controls are part of an IT service like identity management. Application controls are part of a business process.

What are application controls trying to achieve?

Did the right people handle a transaction? Was it recorder correctly? Is it being processed correctly? Are all our transactions are authentic and do they have integrity?
What are “layered controls,” also know in security as “defense in depth”? 
Controls Exercise

• 10 minutes
• Pick a use of computers that someone on your team is familiar with
• Write down all the controls that you associate with it
• Categorize each control as:
  – Preventive, Detective, Corrective
  – General or Application
What is the control environment?

The actions, policies, values, and management styles that influence, and set the tone of a firm's day-to-day activities.
Corporate Leadership

• Senior corporate leadership sets the **tone**
• They are ultimately responsible
• Principals & Policies describe the desired outcomes
• Others may write them, but the board must approve them
Higher Level Management

• Management defines how these objectives will be realized

• Processes, standards and guidelines document the practices and activities are designed to ensure that the organization meet the goals set by senior leadership
Management’s Use of Controls

• Control are put in place to ensure that the Processes, Standards and Guidelines are being followed.

• Therefore, they help mitigate the risk that the behaviors desired by senior leadership will not occur.

• Controls are usually used in combinations so as to ensure that if one fails, the others will correct the behavior.
Monitoring & Audit

- Management should **monitor** their controls to see if the desired behavior is being realized.
- Audits examine the **adequacy and effectiveness** of the controls that an organization has put in place.
The Practical View of Audit
IT Organization Controls

• IT department functional controls
• IT organizational controls
• IT governance & control frameworks
• IT function description controls
• Monitoring and review controls
• IT organization performance measures
A Typical IT Organization

CIO

Office of CIO

Information Systems Development

Quality Assurance

Computer Operations

Technical Support
The Tampa Bay Office Furniture Case

• As teams, take 45 minutes to:
  – Identify all the risks you see in the audit notes (Think Effective, Efficient, Confidential, Integrity, Available, Compliant, Reliable)
  – Identify all the controls you see to mitigate each risk
  – Identify any controls that you think are missing for each risk

• Discuss your findings as a class