Business and Information Process Rules, Risks, and Controls

Internal Control Systems

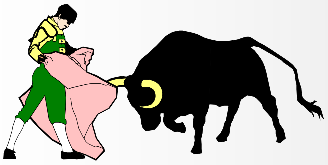
- Internal controls encompass a set of rules, policies, and procedures an organization implements to provide reasonable assurance that:
  - (a) its financial reports are reliable,
  - (b) its operations are effective and efficient, and
  - (c) its activities comply with applicable laws and regulations.
- These represent the three main objectives of the internal control system.
- The organization's board of directors, management, and other personnel are responsible for the internal control system.

Control Environment

- Control environment sets the tone of the organization, which influences the control consciousness of its people. This foundation provides discipline and structure upon which all other components of internal control are built.
- The control environment includes the following areas:
  - Integrity and ethical behavior
  - Commitment to competence
  - Board of directors and audit committee participation
  - Management philosophy and operating style
  - Organization structure
  - Assignment of authority and responsibility
  - Human resource policies and practices

Risk Assessment

- ***Risk assessment*** identifies and analyzes the relevant risks associated with the organization achieving its objectives.
- Risk assessment forms the basis for determining what risks need to be controlled and the controls required to manage them.

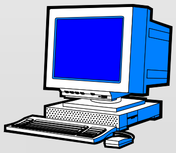


Control Activities

- ***Control activities*** are the policies and procedures the organization uses to ensure that necessary actions are taken to minimize risks associated with achieving its objectives. Controls have various objectives and may be applied at various organizational and functional levels.
- Control Usage - ***Prevent, Detect, and Correct***
  - **Preventive controls** focus on preventing an error or irregularity.
  - **Detective controls** focus on identifying when an error or irregularity has occurred.
  - **Corrective controls** focus on recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

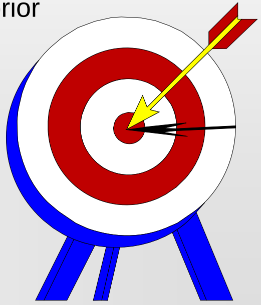
Control Activities

- ***Physical controls*** include security over the assets themselves, limiting access to the assets to only authorized people, and periodically reconciling the quantities on hand with the quantities recorded in the organization's records.
- ***Information processing controls*** are used to check accuracy, completeness, and authorization of transactions.
  - ***General controls*** cover data center operations, systems software acquisition and maintenance, access security, and application systems development and maintenance.
  - ***Application controls*** apply to the processing of a specific application, like running a computer program to prepare employee's payroll checks each month.



Control Activities

- Performance Reviews
  - ***Performance reviews*** are any reviews of an entity’s performance.
  - Some of the more common reviews:
    - compare actual data to budgeted data or prior period data,
    - operating data to financial data, and
    - data within and across various units, subdivisions, or functional areas of the organization.

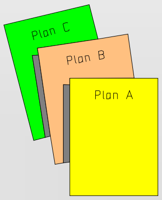


Information and Communication

- The ***information system*** consists of the methods and records used to record, maintain, and report the events of an entity, as well as to maintain accountability for the related assets, liabilities, and equity.
- Requirements:
  - Identify and record all business events on a timely basis.
  - Describe each event in sufficient detail.
  - Measure the proper monetary value of each event.
  - Determine the time period in which events oc
  - Present properly the events and related disclos financial statements.

Information and Communication

- The ***communication*** aspect of this component deals with providing an understanding of individual roles and responsibilities pertaining to internal controls.
- People should understand how their activities relate to the work of others and how ***exceptions*** should be reported to higher levels of management.
- ***Open communication channels*** help insure that exceptions are reported and acted upon.
- Communication also includes the **policy manuals**, **accounting manuals**, and **financial reporting manuals**.



Monitoring

- ***Monitoring*** is the process of assessing the quality of internal control performance over time.
- Monitoring involves assessing the design and operation of controls on a timely basis and taking corrective actions as needed.
  - This process is accomplished by ongoing monitoring activities by management as they question reports that differ significantly from their knowledge of operations.

Traditional Internal Control Environment

Control Environment

Sub-elements of Control Environment

•Management philosophy and operating style
•Organizational structure
•Audit Committee
•Methods to communicate the assignment of authority and responsibility
•Management control methods
•Internal Audit function
•Personnel policies and procedures

***Accounting* System**

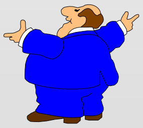
Objectives That Must Be Satisfied

•Validity
•Authorization
•Completeness
•Valuation
•Classification
•Timing
•Posting and summarization

Control Procedures

Categories of Control Procedures

•Adequate separation of duties
•Proper authorization of transactions and activities
•Adequate documents and records
•Physical control over assets and records
•Independent checks on performance



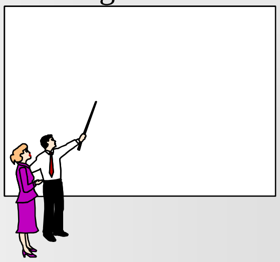
Traditional Control Philosophy

- Much of the traditional accounting and auditing control philosophy has been based on the following concepts and practices:
  - Extensive use of **hard-copy documents** to capture information about accounting transactions, and **frequent printouts** of intermediate processes as accounting transactions flow through the accounting process.
  - **Separation of duties and responsibilities** so the work of one person checks the work of another person.
  - **Duplicate recording** of accounting data and extensive reconciliation of the duplicate data.
  - **Accountants** who view their role primarily as one of independence, reactive, and detective.
  - Heavy reliance on a **year-end review** of financial statements and extensive use of long checklists of required controls.
  - Greater emphasis given to **internal control** than to operational efficiency.
  - **Avoidance or tolerance** toward **advances in information technology**.

Control Concept #1

The perspective of people who develop and evaluate the controls

- **Accountants** must become control consultants with a real-time, proactive, control philosophy that focuses first on preventing business risks, then on detecting and correcting errors and irregularities.



Control Concept #2:

The relationship between risks and specific control procedures

- Use modern IT to achieve the objectives of recording, maintaining, and producing outputs of accurate, complete, and timely information by:
  - **Evaluating the risks** associated with the updated mode of collecting, storing, and reporting data, and
  - **Designing specific control procedures** that help control the risks applicable to the new design.

Control Concept #3

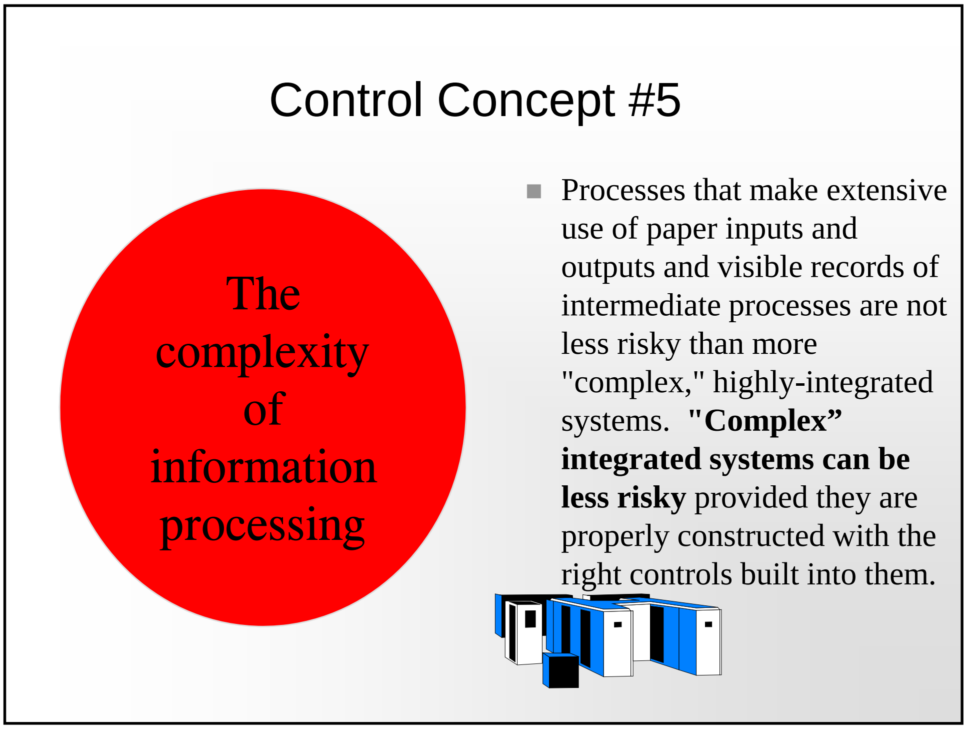
The ability to achieve control and reengineering objectives

- **Tailor control procedures to the business process** so as to improve the quality of the internal control system while enhancing organizational effectiveness.

Control Concept #4

The relationship between information technology and risk

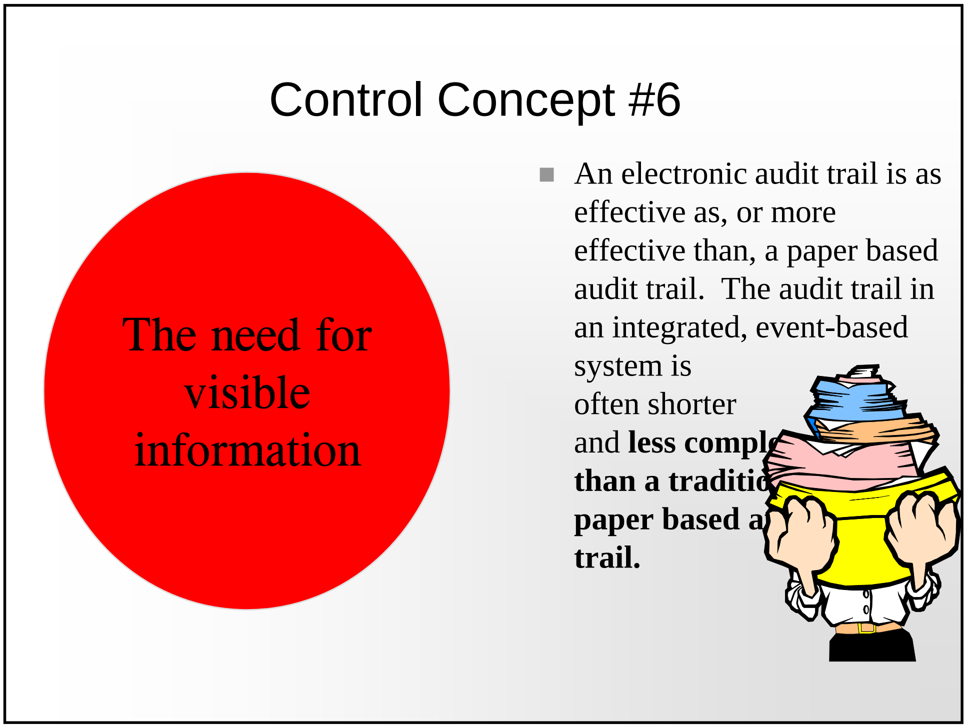
- Accountants must become familiar with IT capabilities and risks and recognize the opportunities IT provides to prevent, detect, and correct errors and irregularities as the business events are executed.



Control Concept #5

The complexity of information processing

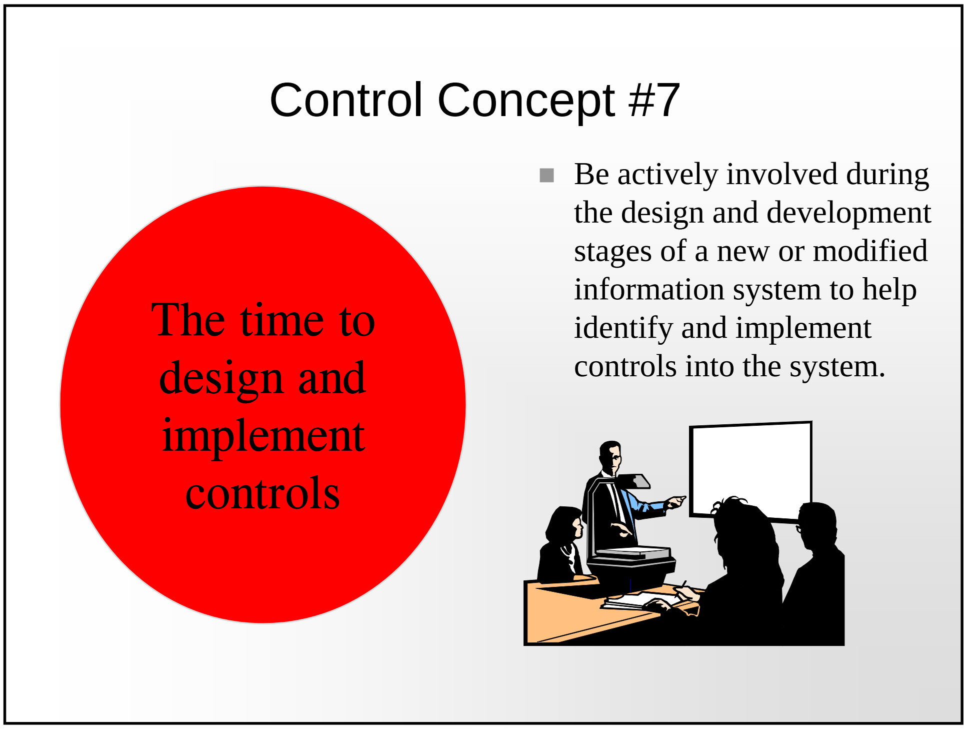
- Processes that make extensive use of paper inputs and outputs and visible records of intermediate processes are not less risky than more "complex," highly-integrated systems. **"Complex" integrated systems can be less risky** provided they are properly constructed with the right controls built into them.



Control Concept #6

The need for visible information

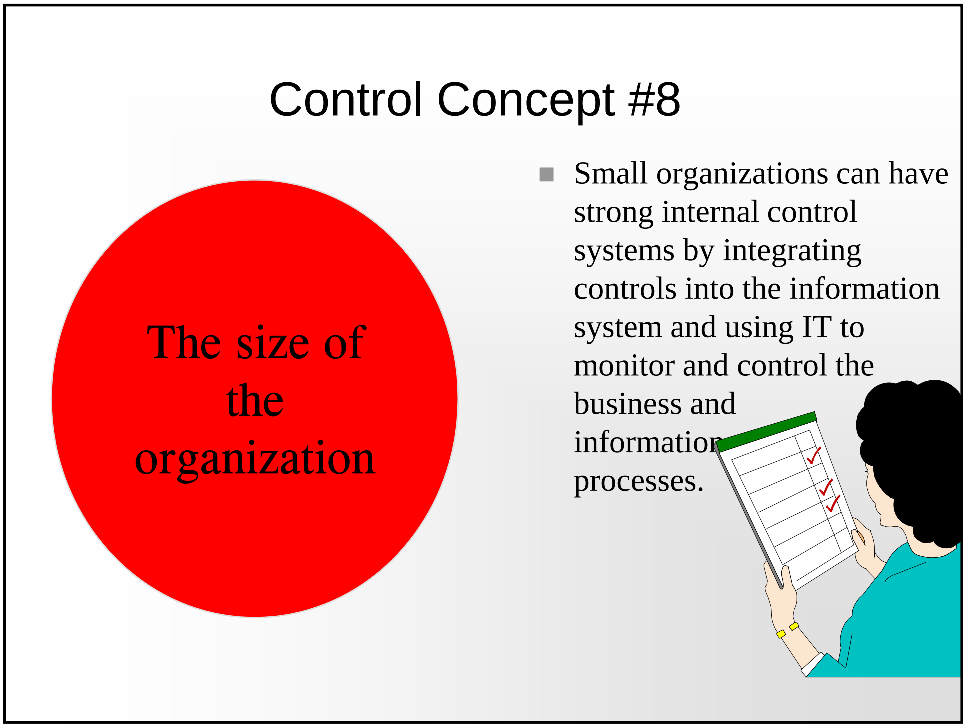
- An electronic audit trail is as effective as, or more effective than, a paper based audit trail. The audit trail in an integrated, event-based system is often shorter and **less compl than a traditio paper based a trail.**



Control Concept #7

The time to design and implement controls

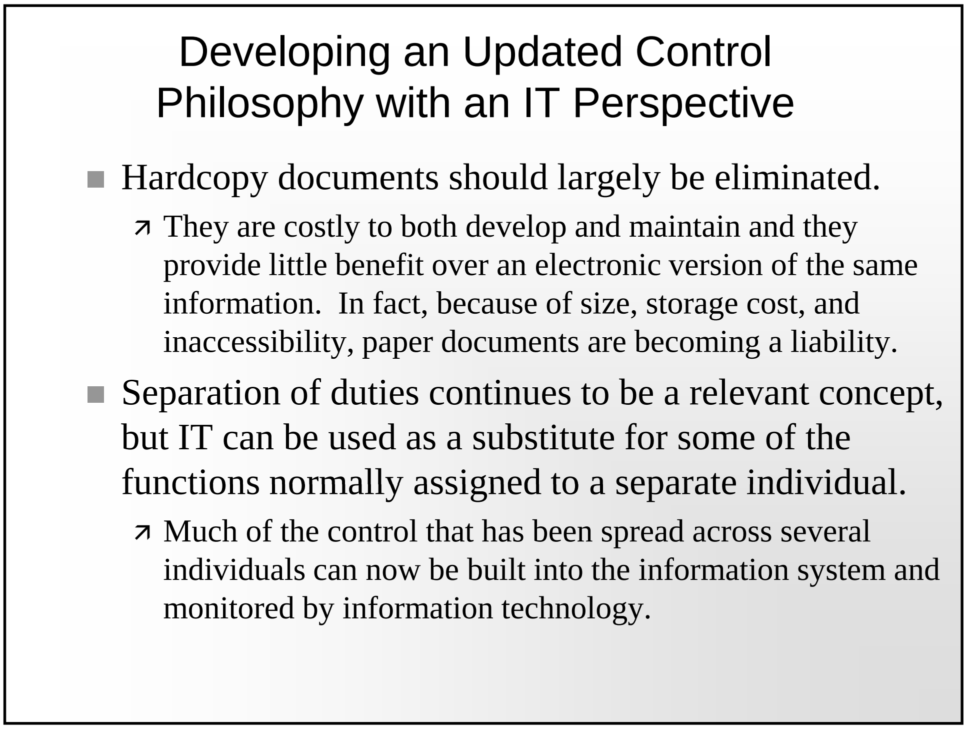
- Be actively involved during the design and development stages of a new or modified information system to help identify and implement controls into the system.



Control Concept #8

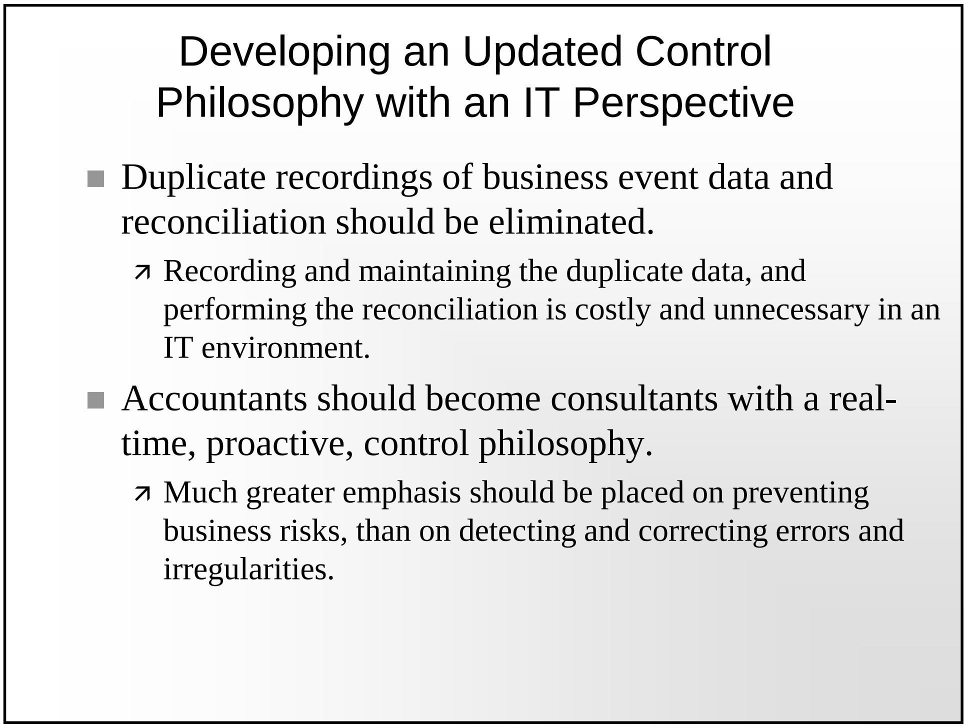
The size of the organization

- Small organizations can have strong internal control systems by integrating controls into the information system and using IT to monitor and control the business and information processes.



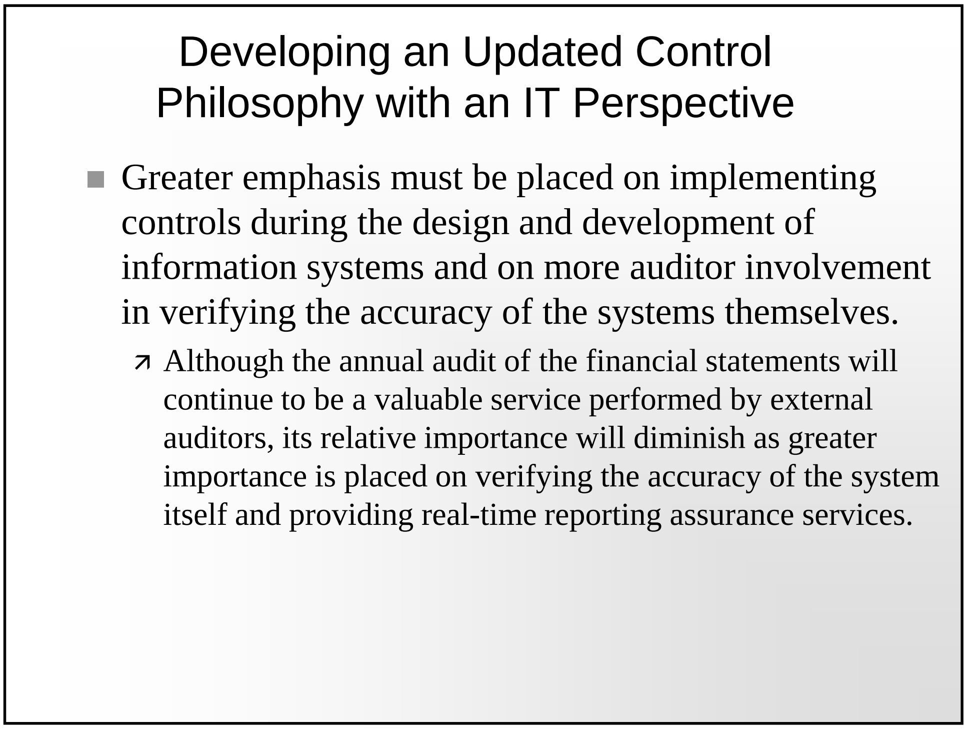
Developing an Updated Control Philosophy with an IT Perspective

- Hardcopy documents should largely be eliminated.
  - They are costly to both develop and maintain and they provide little benefit over an electronic version of the same information. In fact, because of size, storage cost, and inaccessibility, paper documents are becoming a liability.
- Separation of duties continues to be a relevant concept, but IT can be used as a substitute for some of the functions normally assigned to a separate individual.
  - Much of the control that has been spread across several individuals can now be built into the information system and monitored by information technology.



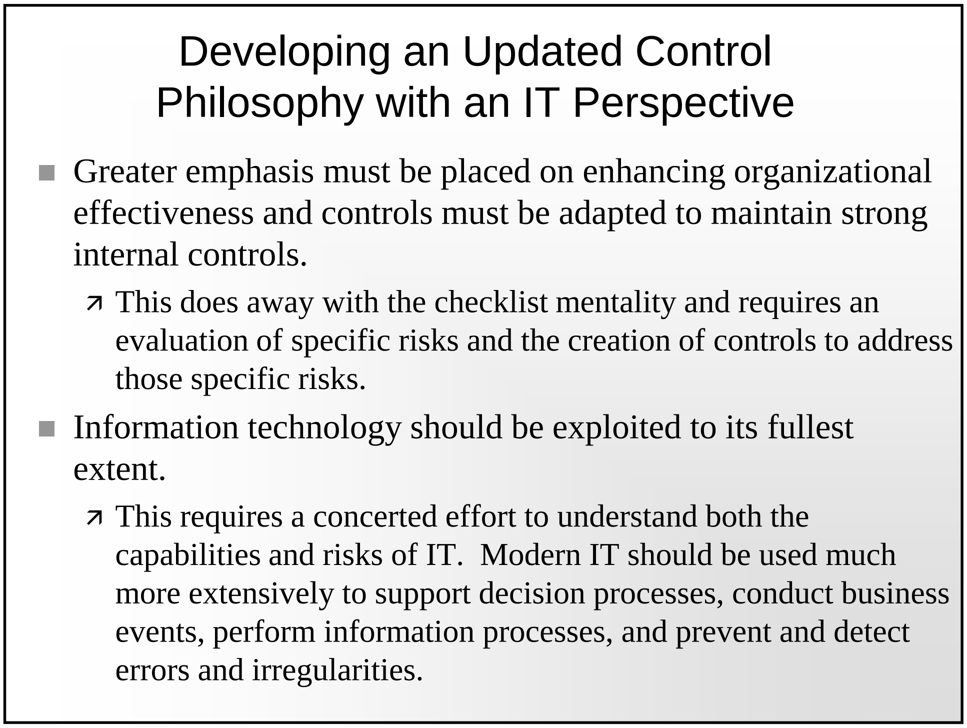
Developing an Updated Control Philosophy with an IT Perspective

- Duplicate recordings of business event data and reconciliation should be eliminated.
  - Recording and maintaining the duplicate data, and performing the reconciliation is costly and unnecessary in an IT environment.
- Accountants should become consultants with a real-time, proactive, control philosophy.
  - Much greater emphasis should be placed on preventing business risks, than on detecting and correcting errors and irregularities.



Developing an Updated Control Philosophy with an IT Perspective

- Greater emphasis must be placed on implementing controls during the design and development of information systems and on more auditor involvement in verifying the accuracy of the systems themselves.
  - Although the annual audit of the financial statements will continue to be a valuable service performed by external auditors, its relative importance will diminish as greater importance is placed on verifying the accuracy of the system itself and providing real-time reporting assurance services.



Developing an Updated Control Philosophy with an IT Perspective

- Greater emphasis must be placed on enhancing organizational effectiveness and controls must be adapted to maintain strong internal controls.
  - This does away with the checklist mentality and requires an evaluation of specific risks and the creation of controls to address those specific risks.
- Information technology should be exploited to its fullest extent.
  - This requires a concerted effort to understand both the capabilities and risks of IT. Modern IT should be used much more extensively to support decision processes, conduct business events, perform information processes, and prevent and detect errors and irregularities.

The Process of Developing a System of Internal Controls

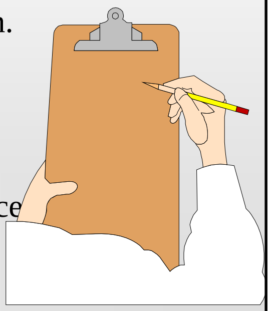
- If you develop a control philosophy based on the key control concepts identified in this chapter, the process of developing an internal control system is rather straightforward:
  - Identify the organization's objectives, processes, and risks and determine risk materiality.
  - Identify the internal control system — including rules, processes, and procedures — to control material risks.
  - Develop, test, and implement the internal control system.
  - Monitor and refine the system.

Risks and Controls in an Event-Driven System

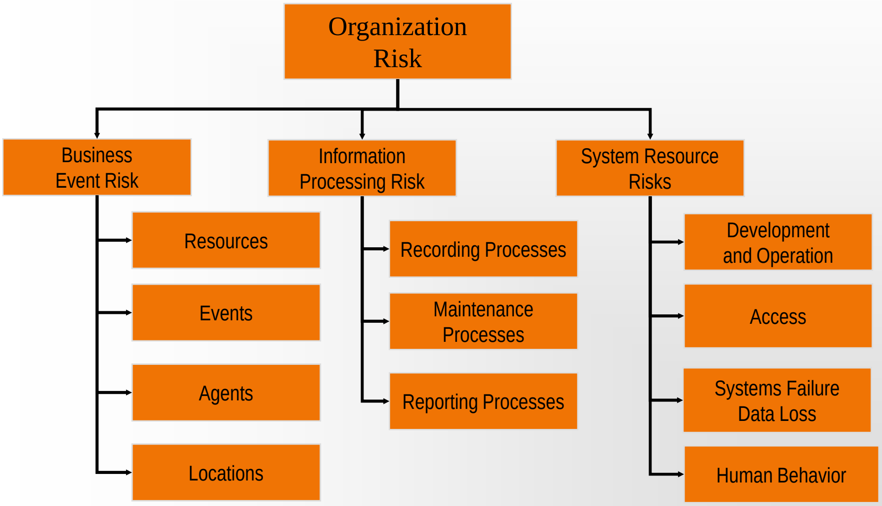
- An event-driven system provides a framework for classifying risks that builds upon what you have already learned about decision, business, and information processes. Acquiring the ability to identify risk requires knowledge of the business organization.
- Business events trigger three types of information processes:
  - ***Recording event data*** (e.g., recording the sale of merchandise).
  - ***Maintaining*** resource, agent, and location data (e.g., updating a customer’s address).
  - ***Reporting*** useful information (preparing a report on sales by product).

Operating Event Risks

- Business event risk results in errors and irregularities having one or more of the following characteristics:
  - ↗ A business event:
    - – occurring at the wrong time or sequence.
    - – occurring without proper authorization.
    - – involving the wrong internal agent.
    - – involving the wrong external agent.
    - – involving the wrong resource.
    - – involving the wrong amount of resource
    - – occurring at the wrong location.



Taxonomy of Business and Information Process Risk



Organization Risk

Business Event Risk

Resources

Events

Agents

Locations

Information Processing Risk

Recording Processes

Maintenance Processes

Reporting Processes

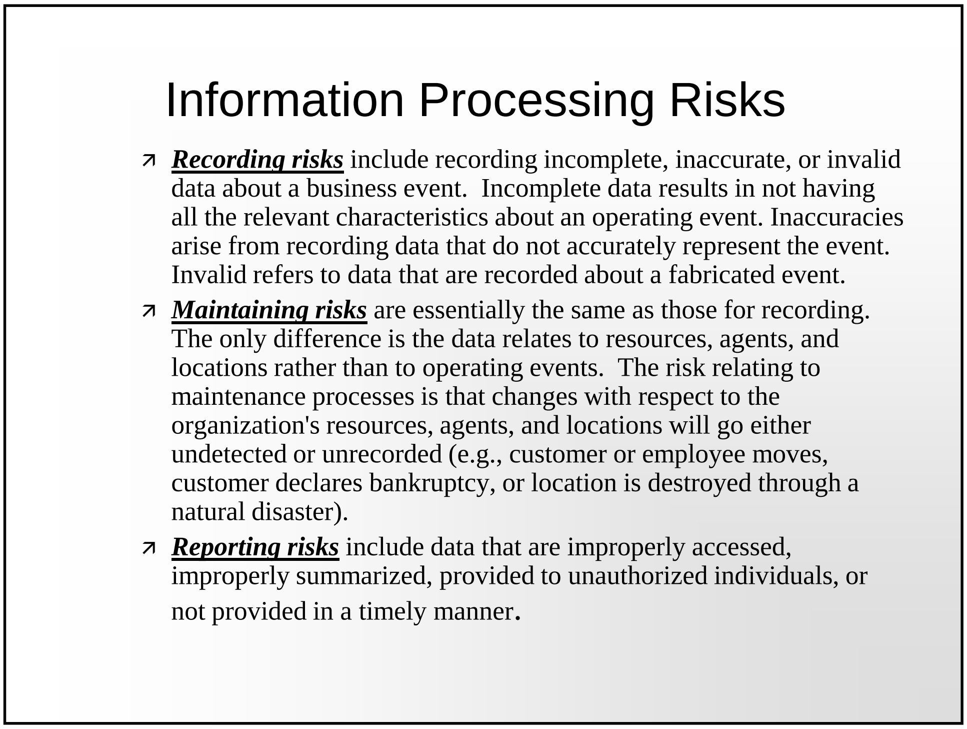
System Resource Risks

Development and Operation

Access

Systems Failure Data Loss

Human Behavior



Information Processing Risks

- ***Recording risks*** include recording incomplete, inaccurate, or invalid data about a business event. Incomplete data results in not having all the relevant characteristics about an operating event. Inaccuracies arise from recording data that do not accurately represent the event. Invalid refers to data that are recorded about a fabricated event.
- ***Maintaining risks*** are essentially the same as those for recording. The only difference is the data relates to resources, agents, and locations rather than to operating events. The risk relating to maintenance processes is that changes with respect to the organization's resources, agents, and locations will go either undetected or unrecorded (e.g., customer or employee moves, customer declares bankruptcy, or location is destroyed through a natural disaster).
- ***Reporting risks*** include data that are improperly accessed, improperly summarized, provided to unauthorized individuals, or not provided in a timely manner.