Information Systems

Security and Control

Objectives

- Describe risks, and controls
- Explain components of an internal control system
- Discuss weaknesses in the traditional control philosophy
- Outline a control philosophy applicable to an informational technology environment
- Describe types of business and information process risks

Risks and Controls

- Risks
  - any exposure to the chance of injury or loss.
- Controls
  - an activity performed to minimize or eliminate a risk.

Threat, Exposure and Risk

- Threat = potential adverse occurrence or unwanted event that could be damaging to the IS or organization
- Exposure = potential money loss due to the threat
- Risk = the chance (probability) that a threat will occur

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.

Risk Assessment ...

- Identify Threats (strategic, operating, financial losses, information errors)
- Estimate Risk (likelihood of occurrence)
- Estimate Exposure (money losses)
- Identify Controls
- Estimate Expected Loss,Costs, and Benefits
- Determine Cost/Benefit Effectiveness

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 Activities

- 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.

General Controls of IS

- Security Plan: Who, What, When, Where
- Segregation of Duties within the Systems Functions
- Project Development Control: scheduling
- Physical Access Controls: access the site and equipments
- Logical Access Controls: access the system
- Data Storage Controls: data protection
- Data Transmission Controls: data encryption

General Controls of IS ...

- Documentation Standards: procedures for data processing
- Minimizing System Downtime: preventive maintenance
- Disaster Recovery Planning: backup, contingent sites
- Protection of Personal Server and Client/Server Networks: inventory and access logs
- Internet Control: intranet, firewall

Application Controls of CIS

- Source Data Controls: accuracy, validity, completeness of data sources
- Input Validation Routines: accuracy, validity input data as it is entered into the system
- On-line Data Entry Controls: validity, integrity of on-line transaction data
- Data Processing and File Maintenance Controls: currency checks, matching, exception reports
- Output Controls: distribution list, shredder

Monitoring Performance

- 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.

Monitoring Performance …

- Effective Supervision
  - assisting, overseeing employees
- Responsibility Accounting
  - budgets, quotas, schedules
- Internal Auditing
  - review the reliability and integrity of financial and operating information
  - appraise the effectiveness of internal control

Traditional Internal Control Environment

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
- External Influences

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.

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 (**through** the system, not **around** it).
  - 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.

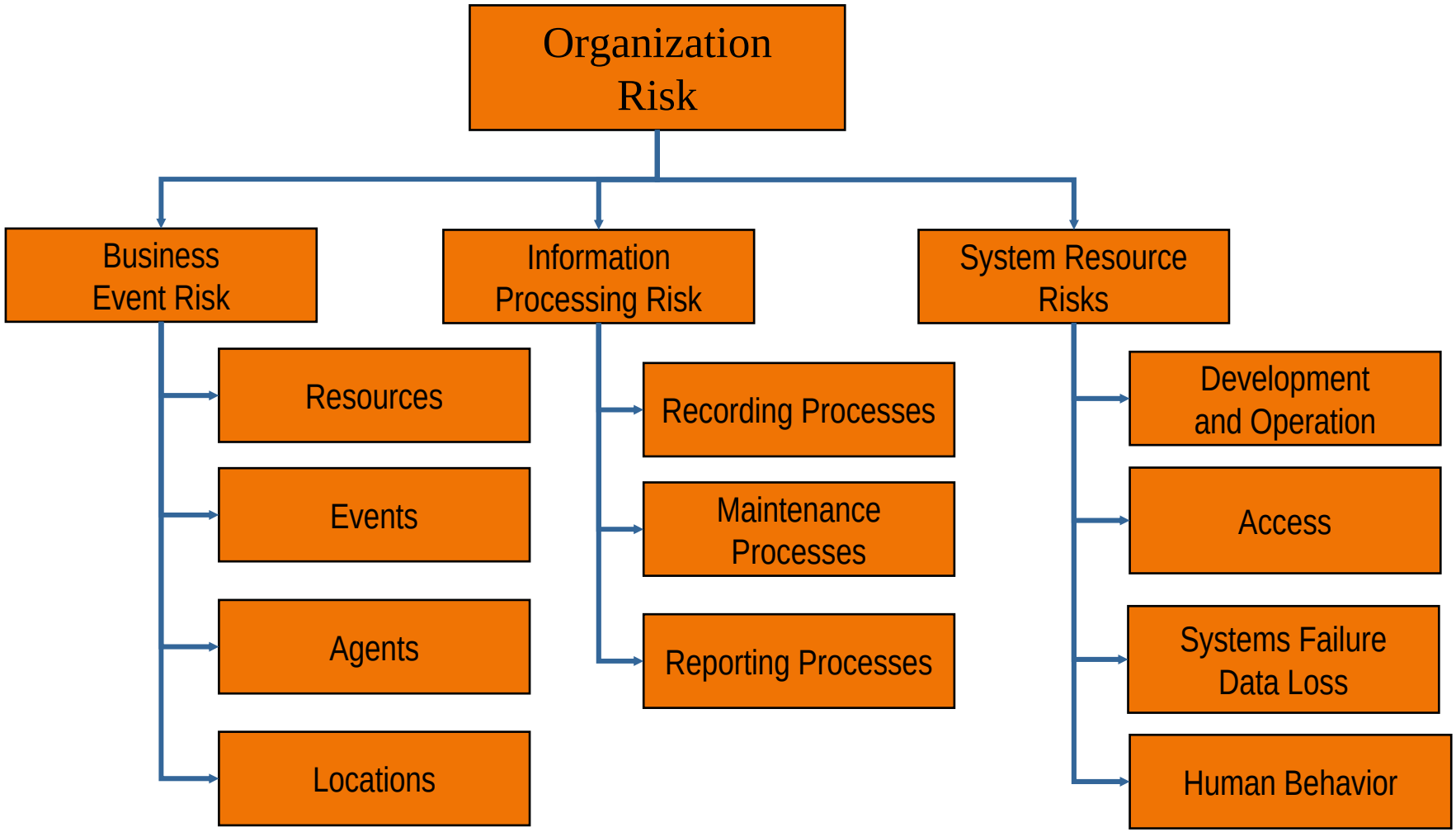
Developing an Updated Control Philosophy with an IT Perspective …

- 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.

Process of Developing a Modern Internal Control System

- 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.

Business and Information Process Risks



Business 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.

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.

Information Processing Risks …

- **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).

Information Processing Risks …

- **Reporting risks** include data that are improperly accessed, improperly summarized, provided to unauthorized individuals, or not provided in a timely manner.