Study Objectives

• Application Control related to Data and Transaction

• Software Development Processes and Quality Standards
Application Control

- What’s an Application Control
- Control practices related to a particular application
  - Control over input data
  - Control over processing, service, transaction
  - Control over output data
Application Control

• What’s an Application Control

• Control practices related to a particular application
  • Control over input data
  • Control over processing, service, transaction
  • Control over output data
How does Application Control Help?

• Data Accuracy
  – Data validity, completeness, accuracy, verifiability, integrity, and reliability

• Processing Accuracy
  – Transaction, service, functional accuracy
Input Controls

A gatekeeper at Input or at Origination Point

• Input Authorization
  – Proper authentication and Authorization in general
  – Online access control
  – Password: unique, sometimes two level
  – Access to data input points such as terminals
  – Source documents: to gather data in organized way like forms
  – Services or transaction: service/access password
  – Batch forms: proper authentication
Input Controls

• Batch Processes
  – Batch forms: proper authentication
  – Batch Controls (items processed as in the batch)
    • Total $ amount
    • # of items in the input
    • # of documents
    • Hash totals: total in batch matches with system calculated sums

• Error handling and Reporting
  – Controls such as
    • By monitoring Transaction logs
    • By Data reconciliation: data received are recorded
    • By using Error correction procedures
    • By validating transmission logs: transmission of receipt of data
  – Errors could be handled in multiple ways
    • Reject the transaction
    • Reject whole batch

Source: Adapted from CISA Review manual, ISACA.
Processing Controls

Ensures accuracy of the processes or procedures while dealing with data.

- Edit Controls – preventive, before processing the data. A number of those discussed in the textbook Exhibit 3.29
  - Sequence Check, Limit Check, Range Check, Validity Check, Reasonableness Check, table look-ups, Existence checks, Key verification, Check digit, Completeness check, Duplicate Check, Logical Relationship Check
Processing Controls

• Processing Controls – Ensure accuracy of the processing of data. Examples include
  – Manual Recalculation: by sampling
  – Edits: validity of the data by the program
  – Run-to-run totals: data read were applied through application processes
  – Programmed Controls: corrective programs
  – Reasonableness of calculated amount: using predetermined criteria
  – Limit Check: against predetermined limits
  – Reconcile of file totals: manually or against independent control files
  – Exception reports: for incorrect data
Processing Controls

• Data File Controls – Ensure authorized processing occurs to the stored data

• Data File control Methods Includes (Exhibit 3.30 textbook)
  – Before and after image, maintenance error reporting and handling, source documentation, internal and external labeling, version usages, data file security, one-for-one checking, prerecorded input, transaction logs, file updating and maintenance authorization, parity checking
Processing Controls

• Data File Types
  – System control parameters: affects working of systems. Should be tightly controlled similar to program changes
  – Standing data: reference data or “master file” such as name, address of partners, product description. Don’t change frequently. Changes to these master files should be managed and approved
  – Master data/balance data: Running balance and totals should not be manually updated, except under tight control and on exception
  – Transaction data: customer transaction data. Changes are controlled through validation checks, exception reports etc.
Output Controls

Providing output data to the Users in a meaningful and consistent way. There are a number of controls:

• Logging of sensitive and critical data
• Negotiable contracts, signatures, etc.
  – should be generated and compared to physical copies
• Report distribution
  – generated reports should be logged and distributed as per plan an access restrictions
  – Applies to electronic or physical report
Output Controls

• Balancing and Reconciling
  – against total
  – Audit trail should be recorded

• Output error handling and retention
  – Reporting on errors
  – Retention requirements and policy, sometimes even legal constraints

• Verification of the receipt of reports
  – logging
SDLC Processes & Quality

• What are some of the standards used to improve quality of Software product, and efficiencies of the team?

  • CMM
  • CMMI
  • ISO 9126
  • ISO 15504
  • COBIT
SDLC Processes & Quality

• What are some of the standards used to improve quality of Software product, and efficiencies of the team?

• CMM
• CMMI
• ISO 9126
• ISO 15504
• COBIT
CMM (Capability Maturity Model of Software)

- Started at Carnegie Mellon University in 1990s
- Five maturity level of software organization, with increased level of maturity
  1. Initial
     - ad-hoc processes
  2. Repeatable
     - The organization can “repeat” software delivery
     - The processes may not be well defined or managed but, delivery is repeatable
  3. Defined
     - Defines standard process
  4. Managed
     - Quantitative managed controls
  5. Optimized
     - Refining the process and optimizing them

CMMI (Capability Maturity Model Integration)

- CMMI less aligned with traditional SDLC model and better aligned with contemporary software development model including Agile and Iterative models.
- Five maturity level of software organization, with increased level of maturity
  1. Initial
     - ad-hoc processes
  2. Managed
     - Processes project based and often reactive
  3. Defined
     - Defines standard process. These are proactive
  4. Quantitatively Managed
     - Quantitative managed controls
  5. Optimized
     - Refining the process and optimizing them
CMMI

Characteristics of the Maturity levels

Level 1: Initial
- Processes unpredictable, poorly controlled and reactive

Level 2: Managed
- Processes characterized for projects and is often reactive.

Level 3: Defined
- Processes characterized for the organization and is proactive.
  (Projects tailor their processes from organization's standards)

Level 4: Quantitatively Managed
- Processes measured and controlled

Level 5: Optimizing
- Focus on process improvement

Source: Adapted from http://en.wikipedia.org/wiki/CMMI
Other Process Improvement Standards

• ISO 9126 – An international standard to assess quality of software products
• ISO 15504 – Software Process Improvement and Capability Determination (SPICE) standard. This is similar to CMM
• COBIT – by ISACA
• Six Sigma – Defect based capability and product maturity
Business Process Reengineering (BPR)

• What is BPR? Why do we need to do BPR?

• Improvement by re-engineering of an enterprise business process

• Often the business processes need to be refined and improved as a result of competitive market pressure, technology, or new discoveries
BPR

• BPR involves
  – Defining the process areas and business function. Often a process area is further decomposed into smaller or elementary processes
  – Redesign, come up with new ways, streamline the process
  – Implement the new process. The new process could have technology or non-technology components
    • IT changes would follow typical SDL processes
    • Users, customer, business impact to be determined, and they would need to get engaged
  – At times Roles and Responsibility of the users of the business process changes with a BPR project
Benchmarking

- Benchmarking is coming up with baseline for a business process
- Benchmarking steps could include
  - Planning: processes to be improved
  - Researching: literature, standard organization
  - Observe: collect data
  - Analyze: the collected data
  - Adopt: in context with an organizational process
  - Improve: continuous improvement against the benchmark
Upcoming Assignments/Tests

1. Quiz 2 (Week 5 – Week 8): Thu 3/17
2. Group Project -2 (Requirements): Thu 3/24 before the class

Questions?
Summary of Today’s Class

• Input Control
• Transaction Control
• Output Control
• CMM, CMMI, ISO
• BPR, Benchmarking
• Focus of the Next Class and Reading
• Questions