Don’t Leave Home Without Your SOX!

Using Function Points to identify and document your company’s application controls for the Sarbanes-Oxley Act of 2002, Section 404

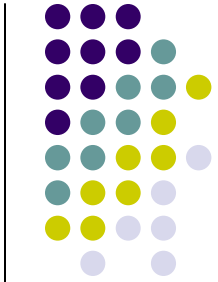
Presented by
Tammy Preuss
CFPS, PMP, Lean Six Sigma Black Belt
AT&T Wireless
Bothell, WA

September 23, 2004

Overview

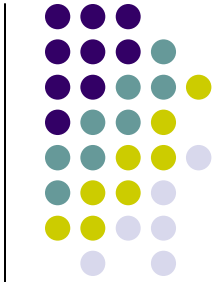
- What is Sarbanes-Oxley & COSO?
- How are companies documenting their internal controls over financial reporting?
- How can using Function Point Analysis assist in identifying control activities that must be documented?

Sarbanes-Oxley Act of 2002



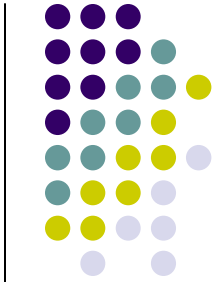
- Signed into law as the “The Public Company Accounting Reform and Investor Protection Act”
  July 30, 2002
  - U.S. Senator Paul S. Sarbanes (D-Md)
    - Former Chairman of Senate Banking, Housing & Urban Affairs Committee
  - U.S. Representative Michael G. Oxley (R-Oh)
    - Republican Congressman representing Ohio’s 4th Congressional District
    - Chair of House Financial Services Committee
- 11 sections
- In response to Enron & WorldCom fraud

Regulatory Agencies



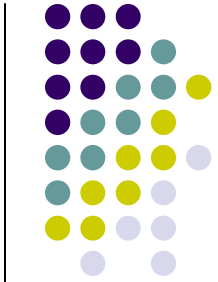
- Public Company Accounting Oversight Board
  - Recommendations to SEC
- Securities and Exchange Commission
  - Approves or rejects PCAOB recommendations.
- For example –
  - PCAOB recommends the Auditing Standard #2: Internal Audit of Internal Control over Financial Reporting Performed in Conjunction with an audit of Financial Statements – 3/9/04
  - SEC Approves 6/18/04

COSO



- COSO = **C**ommittee **o**f **S**ponsoring **O**rganizations of the Treadway Commission
- Treadway Commission = National Commission on Fraudulent Financial Reporting
  - created in 1985 by the joint sponsorship of American Accounting Assn, AICPA, FEI, IIA, Institute of Management Accounts (**note – these are the above mentioned "sponsoring organizations")
- Recommended by PCAOB as having good components for a framework supporting internal controls for Sarbanes-Oxley.

COSO – con't



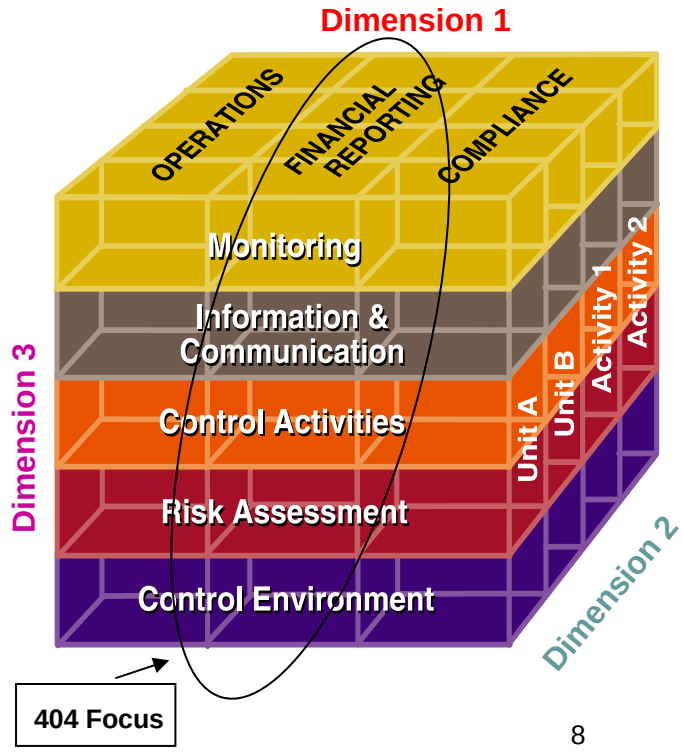
- Purpose – Identify causal factors of fraudulent financial reporting and make recommendations to reduce it's incidence.
  - Report issued in 1987 included recommendations for management and boards of directors of public companies. Included were recommendations that addressed **internal controls.**
- Emphasis on importance of
  - Control Environment
  - Codes of Conduct
  - Competent and involved audit committees
  - Active and objective internal audit function

Definition:
Internal Control = a Process

- Internal Control is
  - A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    - Effectiveness and Efficiency of **Operations**
    - Reliability of **Financial Reporting**
    - **Compliance** with Applicable Laws and Regulations

What is the COSO framework?

- The Integrated Framework uses **three dimensions** that provide management with criteria by which to evaluate internal controls.
- The **first dimension** is objectives, as defined in the internal controls definition
- The **second dimension** is a company-level focus and an process level focus. Internal controls must be evaluated at both the **company-level** and at the **activity or process level.**
- The **third dimension** includes the five components of internal controls that provide the framework for evaluating internal controls over each objective:
  - **control environment**
  - **risk assessment**
  - **control activities**
  - **information and communication**
  - **monitoring**



COSO and information system control activities

- Application Controls
  - apply to the business processes they support and are designed within the application to prevent/detect unauthorized transactions. When combined with manual controls, as necessary, application controls ensure completeness, accuracy, authorization and validity of processing transactions.
- General Computer Controls
  - which apply to all information systems, support secure and continuous operations.

Key Learnings

- Sarbanes-Oxley Act signed into law in 2002
  - Section 404 Requires
    - a report of management on the company's internal control over financial reporting
    - management's assessment of the effectiveness of the company's internal control over financial reporting
    - An auditor to attest to and report on management's assessment
- PCAOB suggests COSO as a good example of an internal controls framework for Internal Control over Financial Reporting.
  - Two broad groupings for Information Systems control activities: Application Controls & General Computer Controls
- Internal Control is a Process

“Laundromat trick. If you lose a sock, simply cannot find its mate... throw the survivor sock into someone else's dryer.”

- www.able2know.com discussion

How are companies documenting their internal controls over financial reporting?

AT&T WIRELESS SERVICES, INC.
AND SUBSIDIARIES

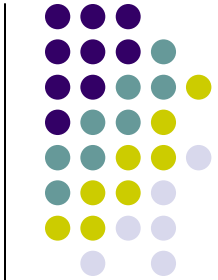
CONSOLIDATED CONDENSED BALANCE SHEETS
(IN MILLIONS, EXCEPT PER SHARE AMOUNTS)
(UNAUDITED)

	AT MARCH 31, 2004	AT DECEMBER 31, 2003
ASSETS		
Cash and cash equivalents	$ 4,067	$ 4,339
Short-term investments	183	202
Accounts receivable, less allowances of $282 and $334	1,994	2,301
Inventories	226	309
Deferred income taxes	288	303
Prepaid expenses and other current assets	415	361
TOTAL CURRENT ASSETS	7,173	7,815
Property, plant, and equipment, net of accumulated depreciation and amortization of $10,828 and $10,146	16,264	16,374
Licensing costs, net	14,499	14,500
Investments in and advances to unconsolidated subsidiaries	1,137	1,169
Goodwill	7,443	7,390
Other assets, net of accumulated amortization of $413 and $378	542	554

What guidelines are used to present a Company's Financial Data?

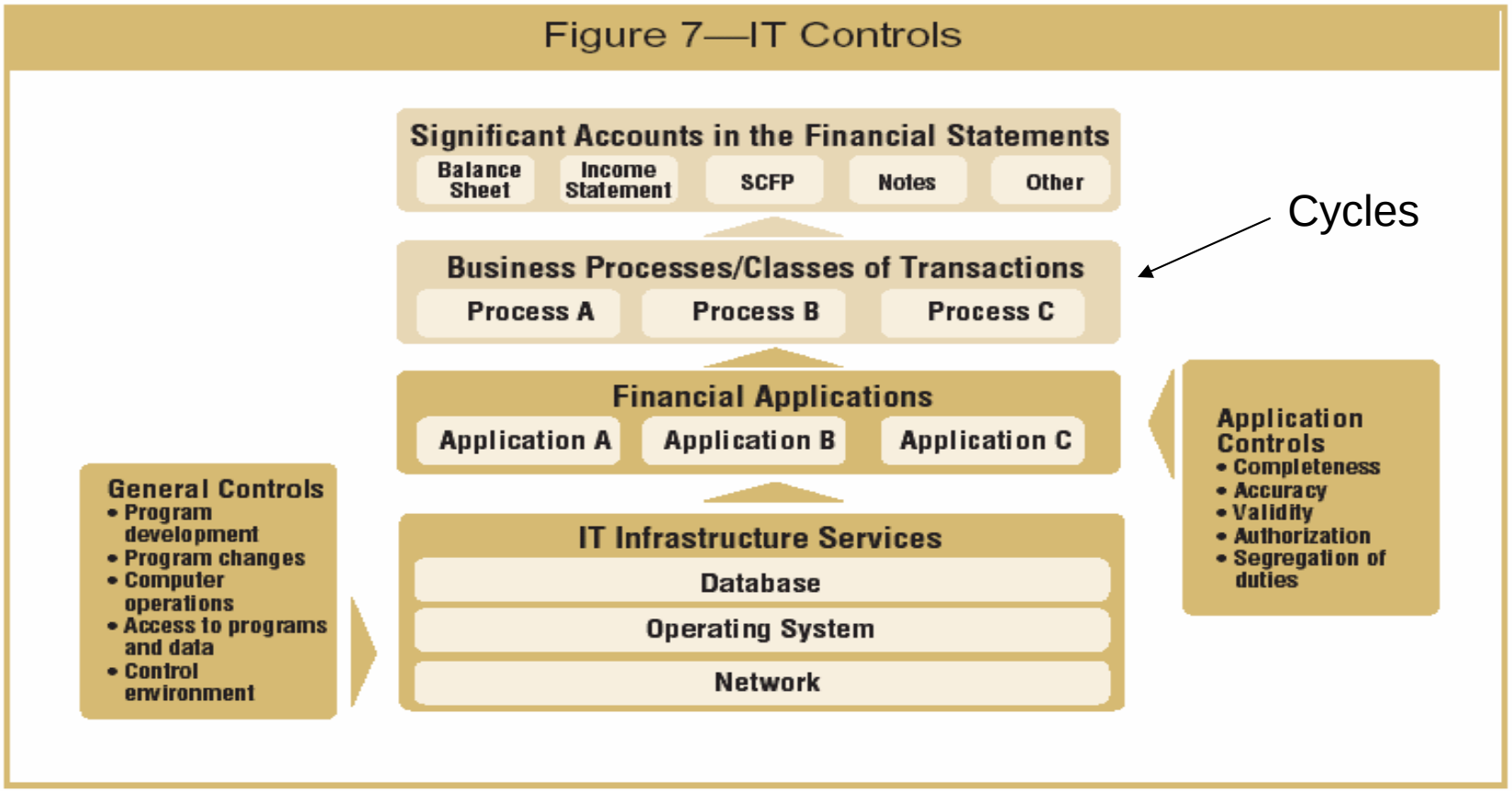
- Financial reporting objectives address the preparation of reliable published financial statements.
- Fair presentation (of Financial Statements)
  - Reflect the underlying transactions and events in a manner that presents the financial position, results of operations and cash flows stated within a range of acceptable limits, that is, limits that are reasonable and practical to attain in financial statements.
  - Inherent in Fair Presentation is concept of financial statement Materiality

Supporting the objectives are Assertions that underlie a company's financial statements



- Completeness
  - Controls exist to ensure actual transactions are not omitted from the records, all transactions are recorded in the correct account; and accumulated totals are correctly transferred to the General Ledger.
- Valuation or Allocation
  - Assets, liabilities, revenues and expenses are recorded at appropriate amounts in accordance with relevant accounting principles.
- Existence or Occurrence
  - Assets, Liabilities and ownership interests exist at a specific date.
  - Recorded transactions represent economic events that actually occurred during a specific period, and should have been recognized in that period, have, in fact been recorded or considered. Therefore there are no unrecorded assets, liabilities or transactions, and no omitted disclosures
- Rights & Obligations
  - The entity has the appropriate rights (such as title). The liabilities of the entity reflect its obligations as of a point in time.
- Presentation & Disclosure
  - Items in the statements are properly described and classified as well as fairly presented in accordance with GAAP and the entity's policies and procedures.

IT has Controls in Financial Reporting too – and the business relies on them!

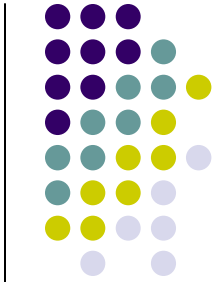


- IT Government Institutes: IT Controls for Sarbanes-Oxley 2004

Which accounts/applications are significant and included in this process?

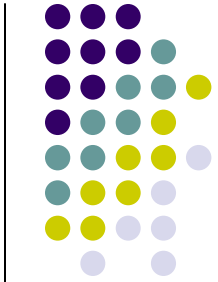
- Does an account/application contribute to financial reporting?
- Is there a risk of financial misstatements and/or internal fraud?
- Do a Risk Assessment on the account/application
  - What is the Impact of it's Failure on Financial reporting?
  - What is the Probability of Error on Financial Reporting?
- Materiality considerations based on
  - Dollar amounts
  - Volume of transactions
    - Work with your external auditor to determine these appropriately.
- All of these are considerations to an application being considered "in-scope" for SOX.

We have our financially significant applications. What happens next?



Objective	Risks	Control Activities	Assertions	Key Control
Transactions are completely and correctly updated to the proper databases	Accounts Payable users may incorrectly key in invoice information which may affect downstream payment processing and the accuracy of A/P balances.	The Payables Invoice entry form validates standard invoice fields such as invoice number, G/L date, and account combinations. The system will not permit a user to enter in a duplicate invoice or G/L date outside the appropriate period. There are no automated restrictions on the invoice amount.	Completeness Accuracy Validity	Yes

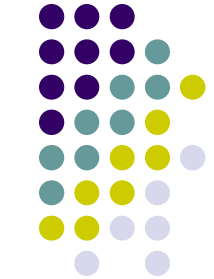
Definition:
Key Control



- Internal Controls (processes), that when operating effectively and taken in aggregate
  - Prevent or Detect
  - And Correct significant deficiencies
  - And satisfactorily address the relevant Financial Statement Assertions…

Source: KPMG SOX 404 Testing

Characteristics of a Key Control



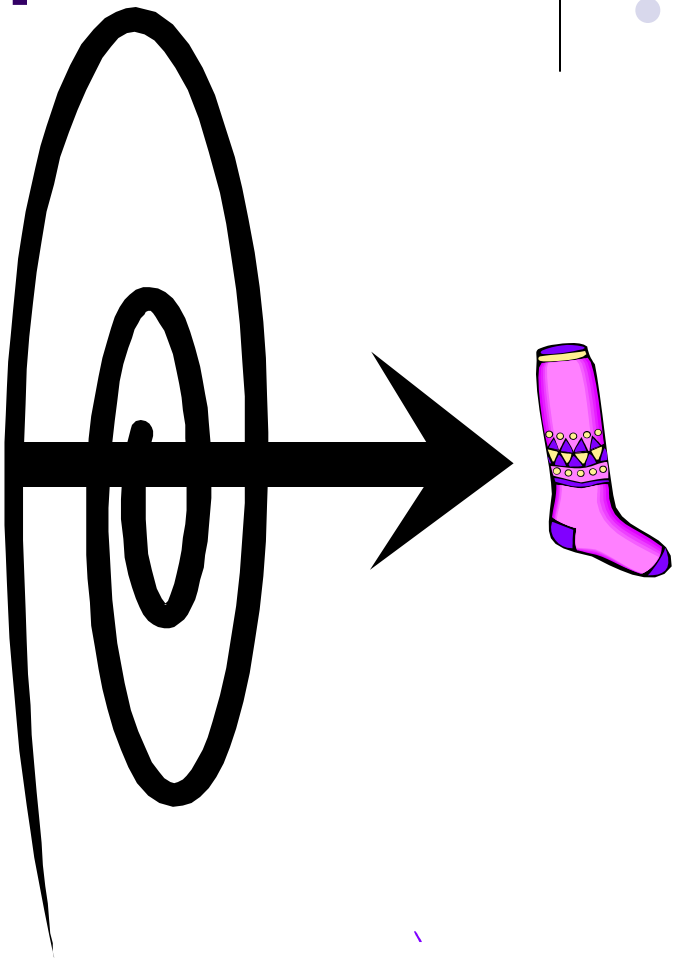
- Management has the most confidence in these controls or considers them the most important controls for mitigating process-level business risks
- For a business process usually consist of both manual and automated controls
- Address the relevant Financial statement assertions
- Address the relevant control objectives
- Can be verified (tested)

Key Learnings

- Financial reporting
  - Supported by business cycles
  - Supported by financial and operational applications
  - Supported by IT Infrastructure
- Risk based on materiality Levels (money & transaction volumes) help determine “in-scope” applications for SOX 404 versus “out-of-scope” applications
- Control Objectives
  - Identify Risks to meeting them
  - Control Activities mitigate those risks
    - The business and IT selected specific activities they are relying on (these are Key)
  - Create Test Plans for Key Controls
  - Test the Key Controls
  - Re-mediate if necessary

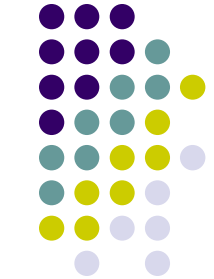
Why do socks disappear?

- There is solid theoretical evidence (which I have unfortunately misplaced) that proves that the explanation can be found in string theory. The rotation of the dryer causes one of those extra dimensions to temporarily unravel and socks are of the correct physical size to slip through the boundary. Their position is unstable however which is why they ultimately appear at inconvenient moments, poking out from under the living room sofa.



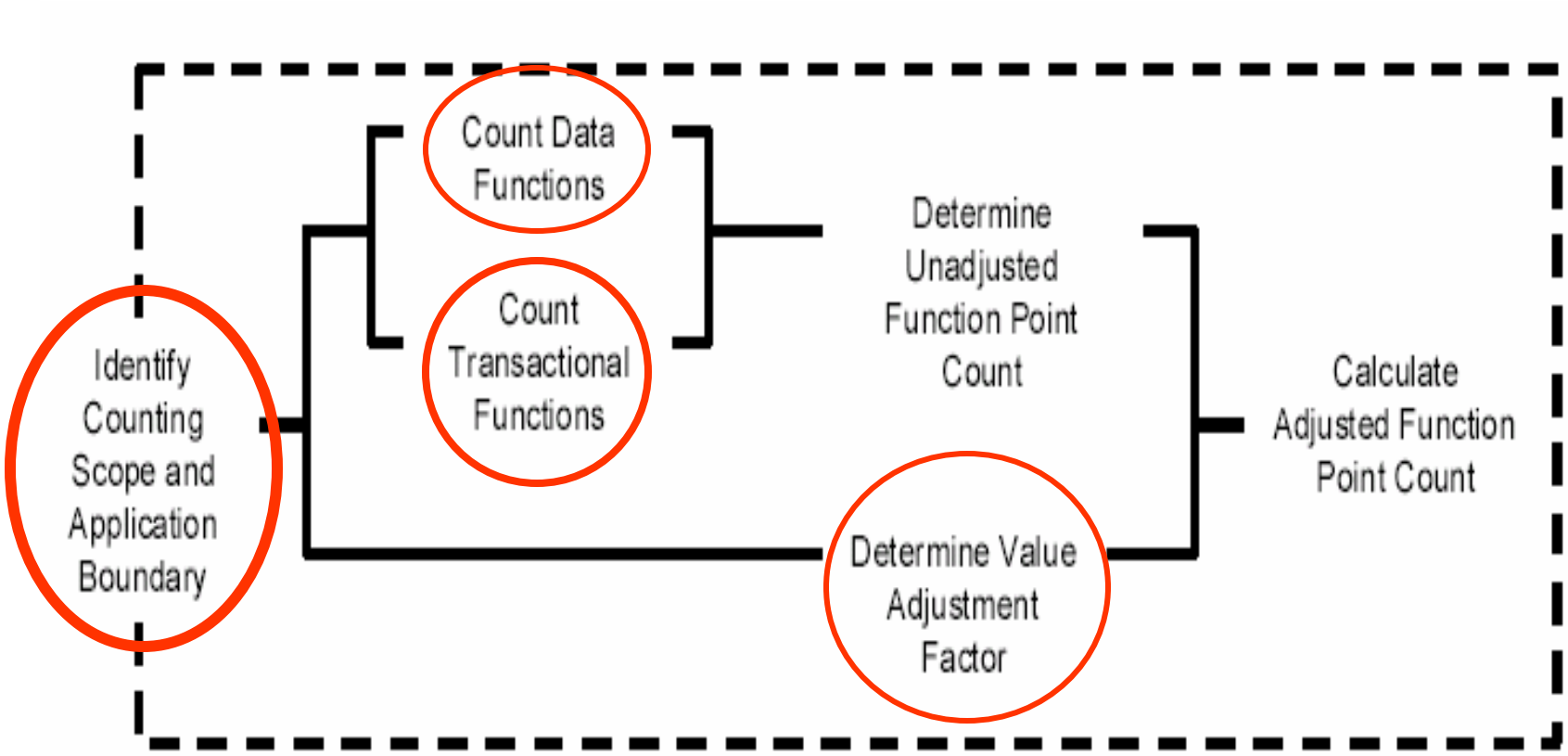
- www.able2know.com discussion

Function Point Analysis - Background

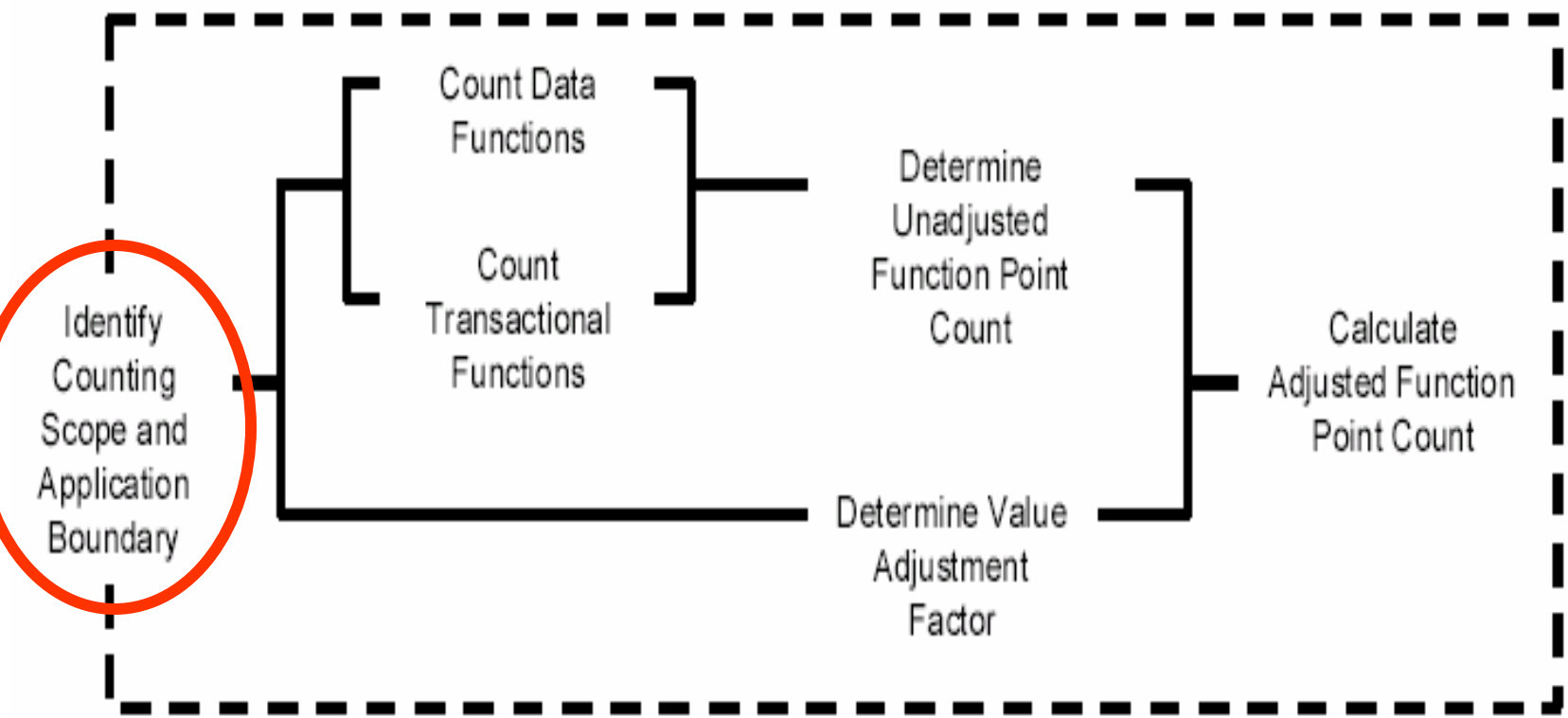


- A method to ‘size’ a software application without regards to technology used
- A ‘normalized’ metric that can be used to measure productivity, rate of delivery, defect density, etc
- Viewing an application from the user’s perspective
  - Business user, System Administrator, another application
  - Does Financial Reporting become a “user”?
- Invented by Allan Albrecht at IBM in 1980’s
- International Function Point User’s Group (IFPUG)
  - Certified Function Point Specialists (CFPS)

We are interested in 4 areas:

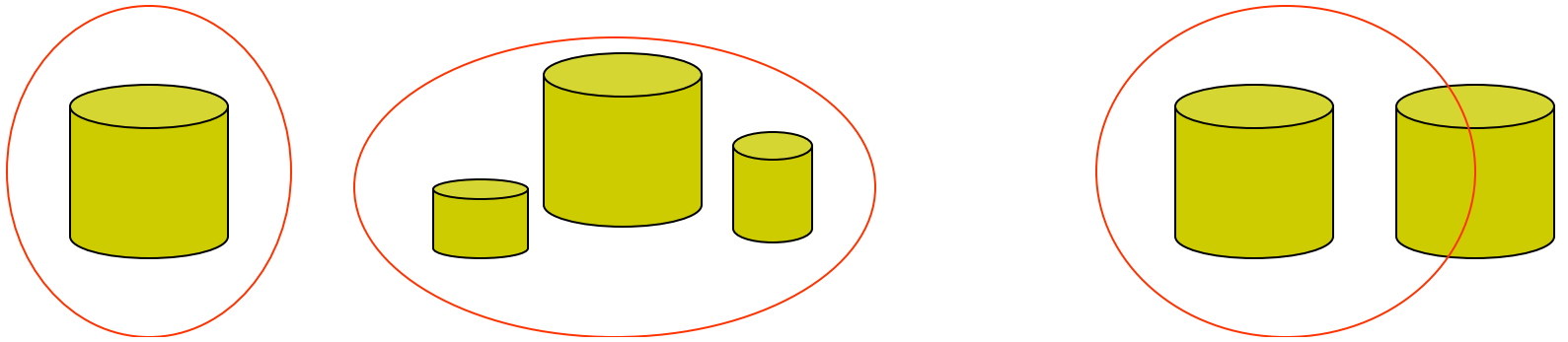


Components of Function Point Count we are interested in for SOX



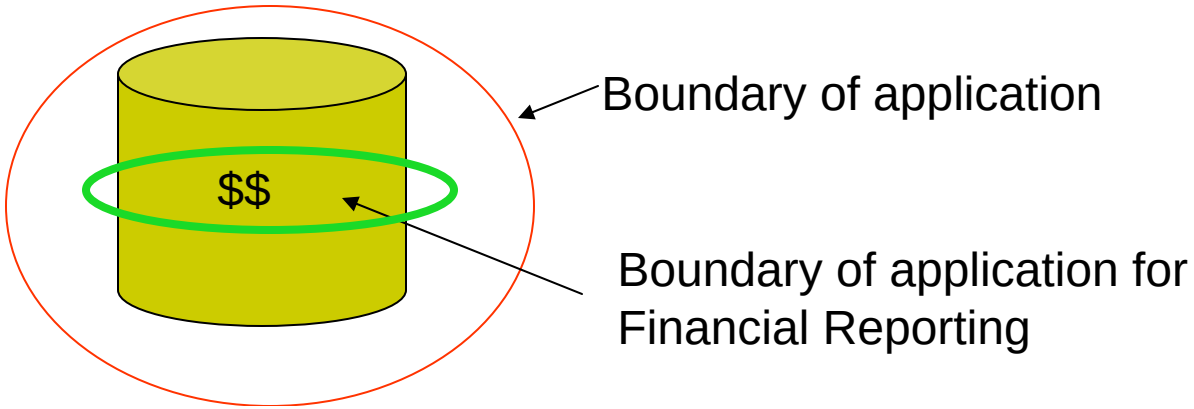
Application Boundary

- Draw boundary around application. This sets the scope of what you are looking at
  - Normal Example: application contained within one server
  - Different but valid examples:
    - Applications which include pre and post processing components – it's not 3 applications; it's 1 big application.
    - Application A maintains (add, change, delete) data in Application B. The parts of Application B maintained by Application A is considered within Application A's boundary



Financial Reporting Boundary

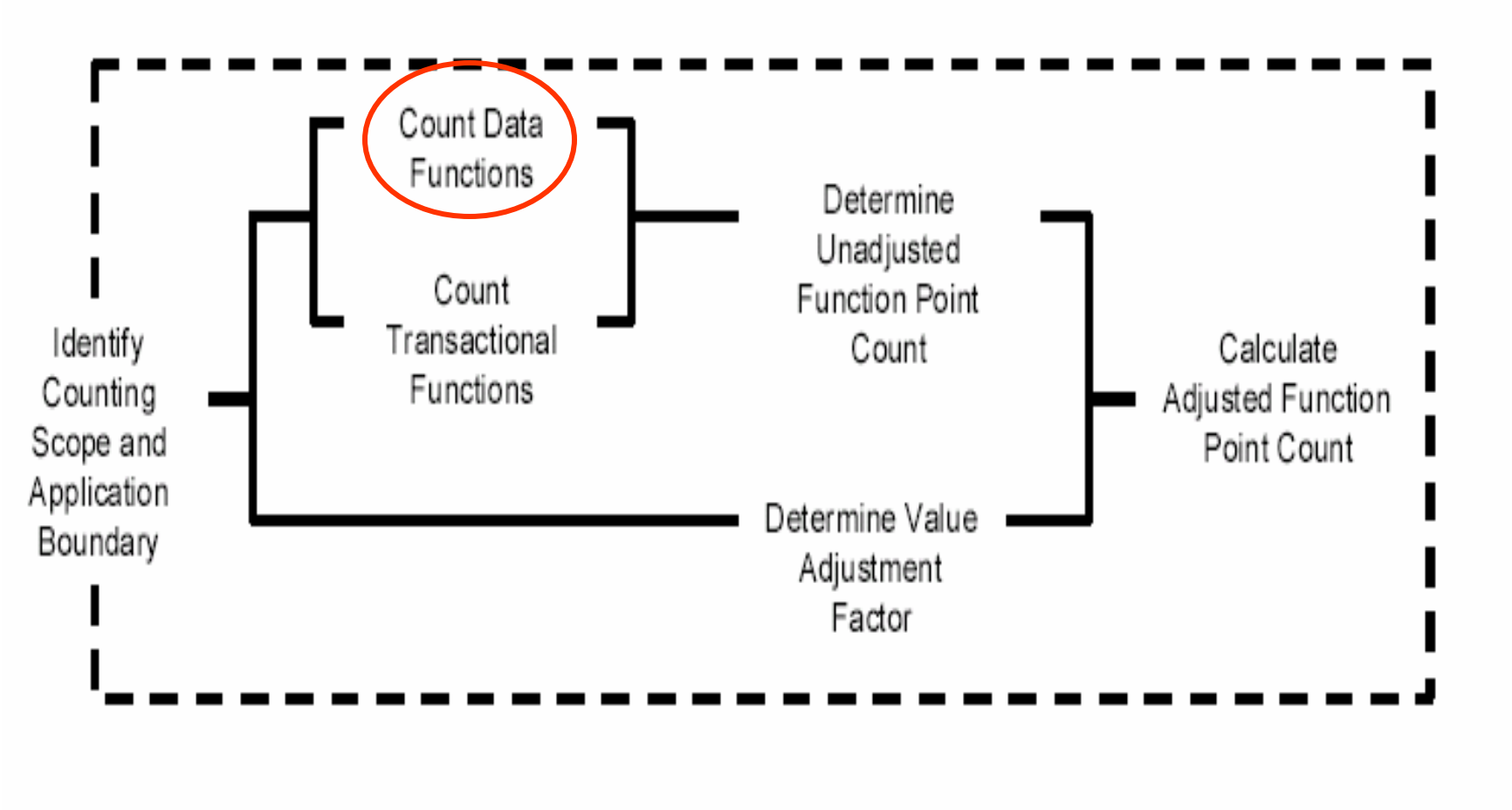
- Let's take that Boundary and refine it for Financial Reporting
  - Easy to do if you already have a baseline function point count
  - Harder if the application hasn't been function point counted – use a Subject Matter expert on the application to assist you.



What % of an application supports Financial Reporting

- Any application where your General Ledger is located (eg Enterprise Resource Planning Applications such as Oracle, SAP, etc),
  - 100%
- Other Financial Reporting applications
  - 75% - 100%
- Any operational application
  - 5% - 75%
  - The farther away from the financial reports your operational applications are, the less percentage of the application needs to be documented for financial controls

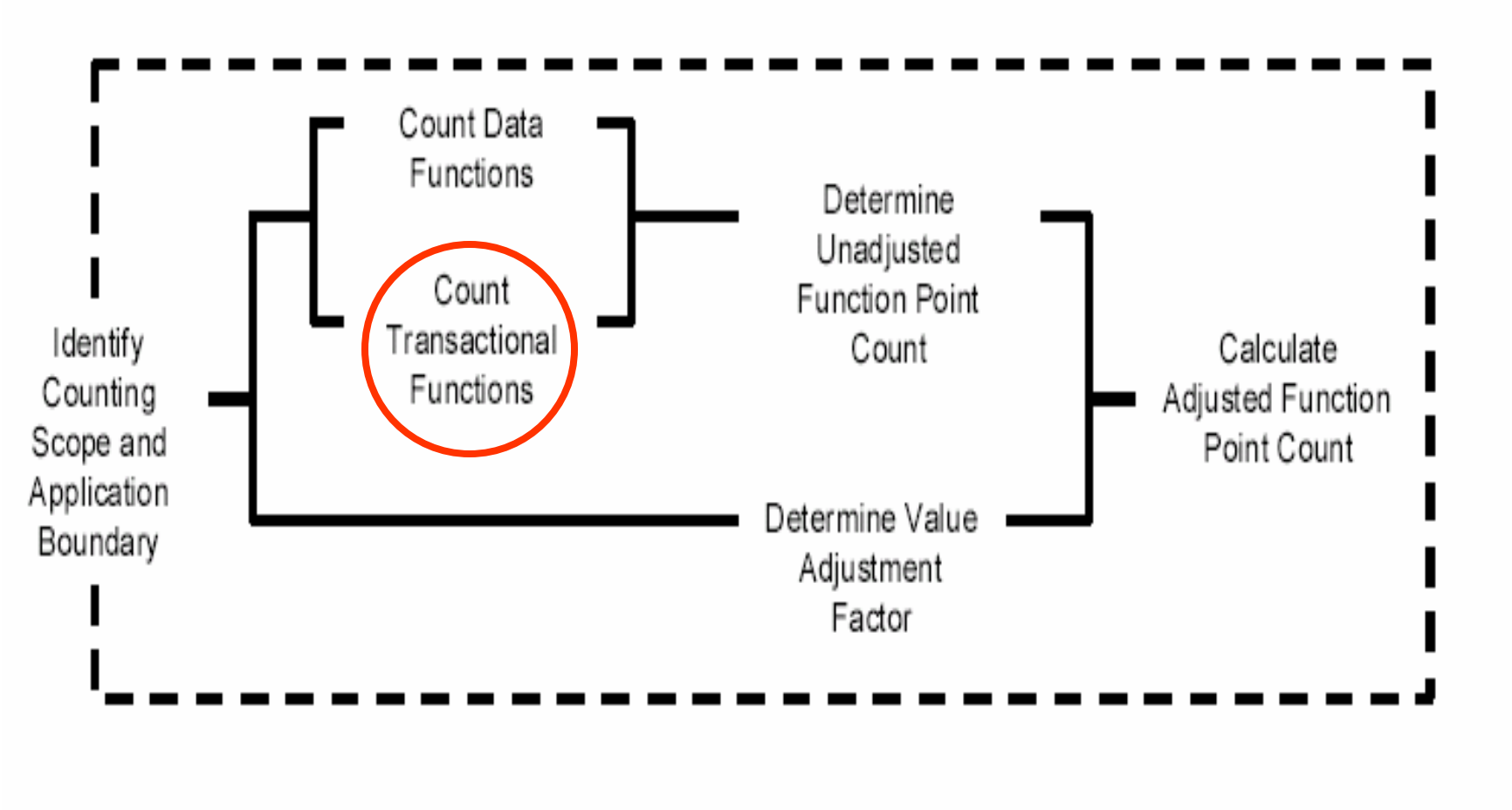
Components of Function Point Count we are interested in for SOX



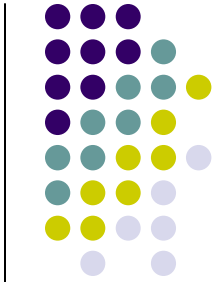
How do internal logical files and external interface files assist in control identification?

- They help identify your financially significant transactions
  - Pay attention to files with obvious monetary data.
    - For example, Credit Card Payment, Account Balance
  - Look at medium and high functional complexity
    - May have more “risk”

Components of Function Point Count we are interested in for SOX



Transactions

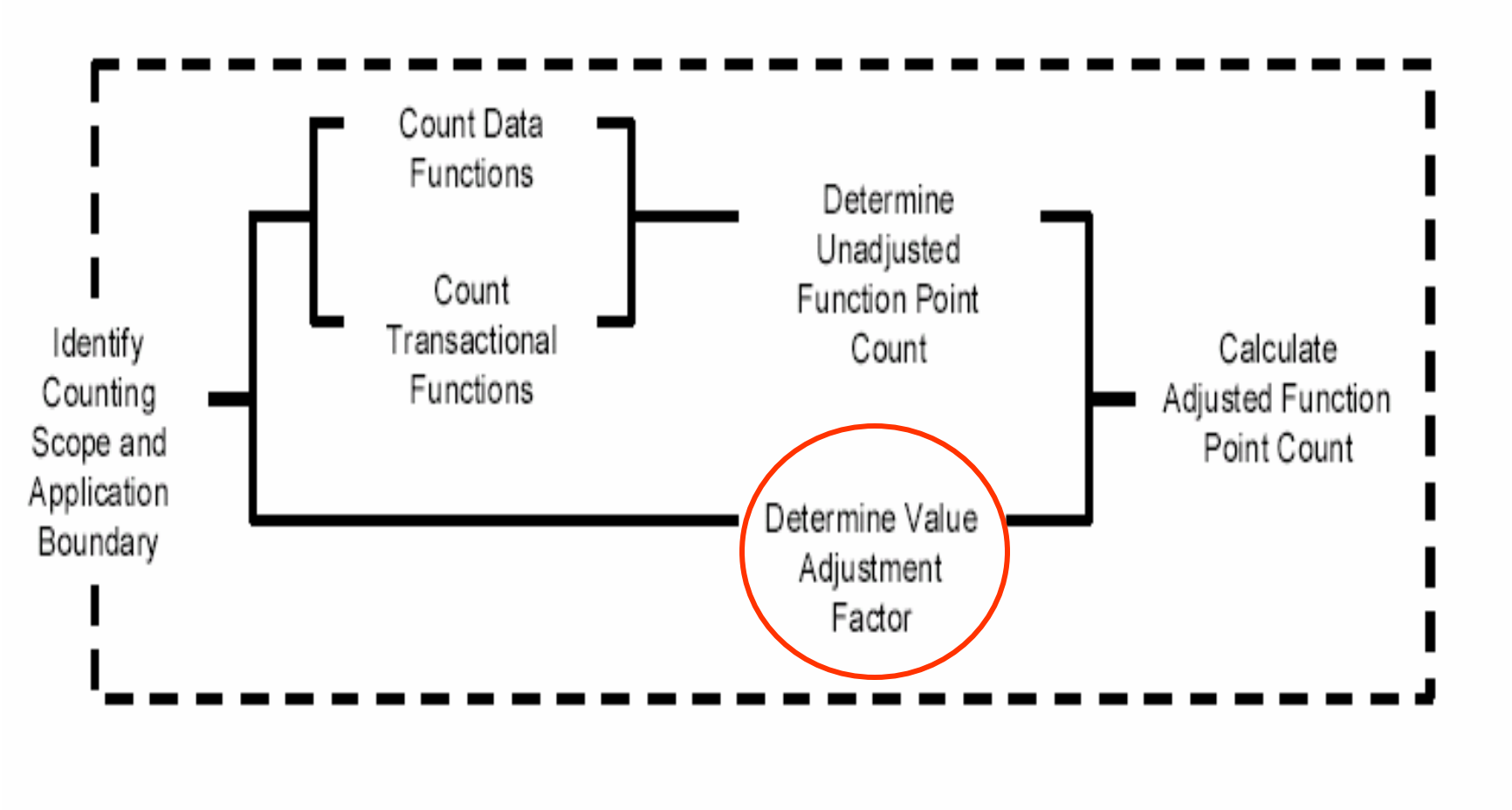


- External Inputs
  - Check input transactions that cross the application boundary and update data
  - Look at the Processing Logic
- External Outputs
  - Check output transactions that cross the application boundary
  - Look at the Processing Logic
  - Look for Derived Data
- External Inquiries
  - For viewing only – can be used to validate controls are working

Using Processing Logic to identify controls

Form of Processing Logic:	Transactional Functional Type: EI	EO	EQ
1. Validations are performed	c	c	c
2. Mathematical formula and calculations are performed	c	m*	n
3. Equivalent values are converted	c	c	c
4. Data is filtered and selected by using specified criteria to compare multiple sets of data	c	c	c
5. Conditions are analyzed to determine which are applicable	c	c	c
6. At least one ILF is updated	m*	m*	n
7. At least one ILF or EIF is referenced	c	c	m
8. Data or control information is retrieved	c	c	m
9. Derived data is created	c	m*	n
10. Behavior of the system is altered	m*	m*	n
11. Prepare and present information outside the boundary	c	m	m
12. Capability to accept data or control information that enters the application boundary.	m	c	c
13. Resorting or rearranging a set of data	c	c	c

Components of Function Point Count we are interested in for SOX



General System Characteristics (look for values of 3-5) to assist in your search for controls

- For Application Controls
  - Transaction Rate (#5)
  - Online data entry (#6)
  - Online update (#8)
  - Complex Processing (#9)
  - Facilitate Change (#14)

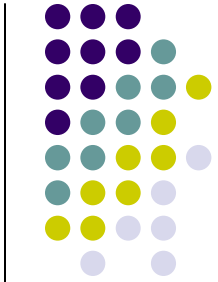
- For General Computer Controls
  - Data Communications (#1)
  - Distributed Data Processing (#2)
  - Performance (#3)
  - Heavily Used Configuration (#4)
  - Installation Ease (#11)
  - Operational Ease (#12)
  - Multiple Sites (#13)

- Not used
  - End-User Efficiency (#7)
  - Reusability (#10)

Key Learnings

- Function Point Analysis can assist in identifying application controls through
  - Data functions
    - Point the way
  - Transactional functions.
    - Show areas of application vulnerability from a financial reporting and fraud perspective.
    - Complexity of transaction (as measured in FP)
    - Processing Logic
  - General System Characteristics

Conclusion



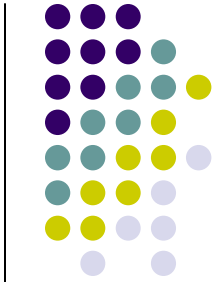
- By utilizing Function Point counting techniques, a counter can quickly identify potential key controls necessary to meet the Act's requirements.
- This in addition to all the areas that a counter can assist you in. For example…
  - Application sizing
  - Software metrics (productivity, defect density)

“Pick up your socks!”

- Contact Information:
  - Tammy Preuss is mother to an active 7 year old. She can be heard frequently shouting this exact phrase throughout her home.

- She can be reached at:
  - tammy.preuss@attws.com
  - 425-288-6705 (work)
  - 714-264-8271 (cell)

Reference Materials



- www.ifpug.org (CPM 4.2)
- www.pcaobus.org (Audit of Financial Systems)
- www.sec.gov/about/laws.shtml#sox2002 (SOX Act)
- www.isaca.org (IT Controls for SOX)
- www.coso.org (Internal Control – Integrated Framework, 2 volumes, July 1994)