

IT Controls in the Financial Accounting and Reporting System

*Sunday, May 20th, 2007
1:00 p.m. – 2:40 p.m.*

*John Sandy, Information Systems Consulting Manager, James Moore & Co., P.L.
JohnS@JMCo.com*

*Chris A. Meyers, Internal Technology Services Manager, James Moore & Co., P.L.
ChrisM@JMCo.com*

Infrastructure



Application's Control

John Sandy, A Really Great Guy



What???
Objective, Goal, Purpose ...

Ensure the proper
recording & reporting
of financial information



Why go to the trouble?

DATA IS A BUSINESS'
GREATEST ASSET!



Guidelines

- Basis – SAS 94
- Software – Varies



Axiom, Truism, with Procedure

Typically what makes the
process **stronger**
makes the process **longer**

Is the **strength** worth the
length?



Application Control's – 4 Areas

1. Input
2. Processing
3. Output
4. Security



Input Controls

Procedures used for:

1. Authorizing data
2. Assuring completeness and accuracy of data at:
 - **Initial** recording and
 - Conversion to machine readable form.
3. **Assure rejected data is properly re-entered.**



Input Controls

(ensure proper R&R)

- I.D. Source Documents
 - stamp, initial, etc.
- **Standard Input forms/stamp**
- Verification
 - Customer #s, Vendor #s
- **Supervisory Override**
 - Recorded and reviewed



Input Controls

(ensure proper R&R) (cont')

- **Restriction on Master File changes**
 - Reviewed/notify originator
- Standard Menu screens
- Use batch totals, record counts, other control totals
- Exception reports
- **Designee to handle errors**
 - Log, review, follow-up



Process Controls

1. The completeness and accuracy of processed data
 - Includes database and table information
2. **Data files changed only through normal processing** (SQL & EXCEL)
3. Prevention/processing incorrect files
4. Highlighting system administration errors
5. Establishment of recovery procedures in the event of failure



Processing Controls

(ensure proper R&R)

- Programming checks:
 - Sequence
 - Incomplete
 - Reasonableness tests
 - Comparison of codes
 - Account #s, job #s
 - Alpha/Numeric
- Comparison Input vs. Control



Processing Controls

(ensure proper R&R)

- Manual checks of external labels
- **Review system administration log for error messages caused by system administration action**
- Restore procedures



Output Controls

1. Assure output is distributed to authorized personnel
2. Output scanned/compared to original documents
3. Output contains sufficient information to permit detection of errors and the handling of subsequent corrections
4. **Error and discrepancy reports are produced, kept, and reviewed by proper personnel – assure corrections made**
 - Was-Is reports



Output Controls (cont')

5. Output totals are reconciled with input and processing control totals
6. **Appropriate procedures for handling**
 - Rejected transactions
 - Reported errors or discrepancies
 - Unexplained reconciling differences
7. **Backups properly identified**



Security

1. Adequate physical security
 - Castle
2. Programmers restricted access to live operation
3. Prevent testing of new programs on live data



Security (cont')

4. Databases:

- a) Restrict access to application processing database or tables to authorized personnel only
- b) Changes logged and adequately reviewed

5. Passwords:

- a) Confidential and unique (MS complex)
- b) Changed at regular intervals
- c) Create roles
- d) Promptly cancelled for terminated employees



Security (cont')

6. Data Dictionary

- All data has been classified and assigned the appropriate risk ranking that will support and provide evidence for the use of implemented security controls



IT Controls in the Financial Accounting and Reporting System

General Controls from a SAS94 perspective

Chris A. Meyers, A somewhat less of a great guy than John Sandy.

ITS Manger
James Moore & Co., P.L.
ChrisM@JMCo.com



General Controls

General controls relate to the IT infrastructure & processes as opposed to individual accounting applications. We will be examining these controls from a SAS94 perspective (ie. how IT related controls affect the financial audit)



SAS94 General Controls – process

1. Need established (complex?)
2. Work order created by PIC
3. Scheduling / planning meeting
4. Preliminary work: contacts, network information, etc.
5. Interviews
6. Testing (checklists via inquiry & observation, additional testing per work order)
7. Internal report to PIC
8. Additional reports (if requested)



General Controls – 6 Areas

1. Organization
2. Access
3. Application development
4. System software
5. Operational
6. Disaster recovery / contingency planning



Organizational Controls

1. IT department independence?
2. Separation of duties between programmers, system admins, and users?
3. Annual vacation for IT personnel? During absence, someone else must perform their duties.
4. IT personnel cannot initiate master file changes.



Access Controls

1. Do physical access controls exist?
2. Application access controlled (via network and/or application itself)? Password policies?
3. Programmers restricted from life data.
4. Users restricted from programming environment.
5. Remote access strictly controlled for users, vendors, etc.
6. New internal network controls...
 1. data traffic security based on sensitivity
 2. intrusion detection
 3. data classification by risk



Application Development Controls (ugh!)

This is where we see MOST control violations!

1. Established procedures exist...
 1. Application Development?
 2. Prevent unauthorized changes?
 3. User & internal audit team involvement?
 4. To control movement of new/modified programs into testing or production?
2. Formal standards for DOCUMENTATION



System Software Controls

(includes OS, db apps, security software, file management software, etc.)

Only applies if organization's personnel "have the technical expertise and tools to develop or modify system software."

1. These personnel are prevented from having a detailed understanding of key accounting application and controls.
2. Controls similar to Application Development exist.
3. ALWAYS APPLIES: Critical software patches must be applied per vendor specifications.



Operational Controls

(primarily affecting system administrators)

1. System admins must...
 1. log their activities (manual or automated). Logs must be reviewed.
 2. report system failures / unusual incidents.
 3. have appropriate instruction/process manual available.
 4. have compliance monitored.
 5. have background checks.
2. Appropriate controls for outside third-party access such as...
 1. vendor must request access (one-time use username/password).
 2. vendor does not have "automated" access but must be specifically authorized each time.
 3. call back access.



Disaster Recovery / Contingency Planning

1. Appropriate backup procedures exist?
2. Test restores of data!!!
3. Off-site storage of data (e.g. tape, DRP, documentation, etc).
4. DR/CP plans EXIST? And have been tested?



Software used

(GC side of the house...)

1. CCH Engagement
2. PPC's e-Tools
3. LANguard Network Security Scanner
4. Network Stumbler
5. Ethereal
6. Ping Plotter
7. Port Flash



Q & A


