Auditing Applications

ISACA Seminar: February 10, 2012

AGENDA

- Planning
- Objectives
- Mapping
- Controls
- Functionality
- Tests
- Complications
- Financial Assertions
- Tools
- Reporting

PLANNING

- Consideration / understanding of the control environment

- Consideration of how audit arose
  - From audit plan?
  - Ad hoc?
  - What is driving the need for THIS audit?

PLANNING

Key risks should be defined in planning and monitored with adjustments throughout.

- Which risks were identified through audit source?
- Where are controls likely strong and weak?
- What is the relationship of the audit objectives, scope and procedures?

	Inherent Risk	Control Risk	Assessed Risk
Risk	(Sub-Categories as Applicable)	Control Risk	Residual / Assessed Risk
Invalid, inaccurate, and/or incomplete data may cause errors in reporting or in accounting.			
Unauthorized or unintended changes to systems may cause errors in reporting or in accounting.			
Unauthorized access may lead to unauthorized changes to systems and data, causing errors in reporting or in accounting.			
Invalid, inaccurate, and/or incomplete systems processing may cause errors in reporting or in accounting.			

PLANNING

- Pre-implementation or post-implementation?
  - Pre-implementation audits tend to be proprietary

- What is in scope?
  - Interfaces
  - Source systems
  - Target systems
  - Infrastructure / component

Risk	Scope of Systems
Invalid, inaccurate, and/or incomplete data may cause errors in reporting or in accounting.	XYZ Oracle Database XYZ ETL Software
Unauthorized or unintended changes to systems may cause errors in reporting or in accounting.	XYZ Oracle database XYZ ETL Software XYZ Job Scheduler
Unauthorized access may lead to unauthorized changes to systems and data, causing errors in reporting or in accounting.	Input: Source File Network Drive(s) Processing: XYZ Oracle Database, XYZ ETL Software, XYZ Job Scheduler Output: Extracts Network Drives
Invalid, inaccurate, and/or incomplete systems processing may cause errors in reporting or in accounting.	Documentation: All In-Scope Systems Processing / Errors: XYZ ETL Software and XYZ Job Scheduler

- Evaluate team for sufficient expertise to perform the audit

OBJECTIVES

- Efficiency
- Effectiveness (information requirements)
- Compliance
- Alerts (if necessary)
- Financial reporting
- Proprietary

Risks, Scope, and Procedures					
Ref.	**Risk**	**Risk Area**	**Objective**	**Audit File Reference**	**Procedures**
1	Invalid, inaccurate, and/or incomplete data may cause errors in reporting or in accounting.	Data Integrity	Evaluate data integrity checks and controls between inputs and outputs.	F.1.1	
2	Unauthorized or unintended changes to systems may cause errors in reporting or in accounting.	Change Management	Evaluate changes to - related systems for appropriate approvals, testing, and segregation of duties.	F.1.2	
3	Unauthorized access may lead to unauthorized changes to systems and data, causing errors in reporting or in accounting.	Security	Assess logical access to systems.	F.1.3	
4	Invalid, inaccurate, and/or incomplete systems processing may cause errors in reporting or in accounting.	Operations	Evaluate system processing and documentation for appropriate guidance on development and support, system processing / job scheduling, and error identification and resolution.	F.1.4	

MAPPING

Tool for thorough understanding and adequate considerations for audit procedures throughout the steps from planning to reporting

- Relevant IT Components/Description
- Business Owners & System Administrators
- Change Management Process/Owner
- Security Administration Process/Owner

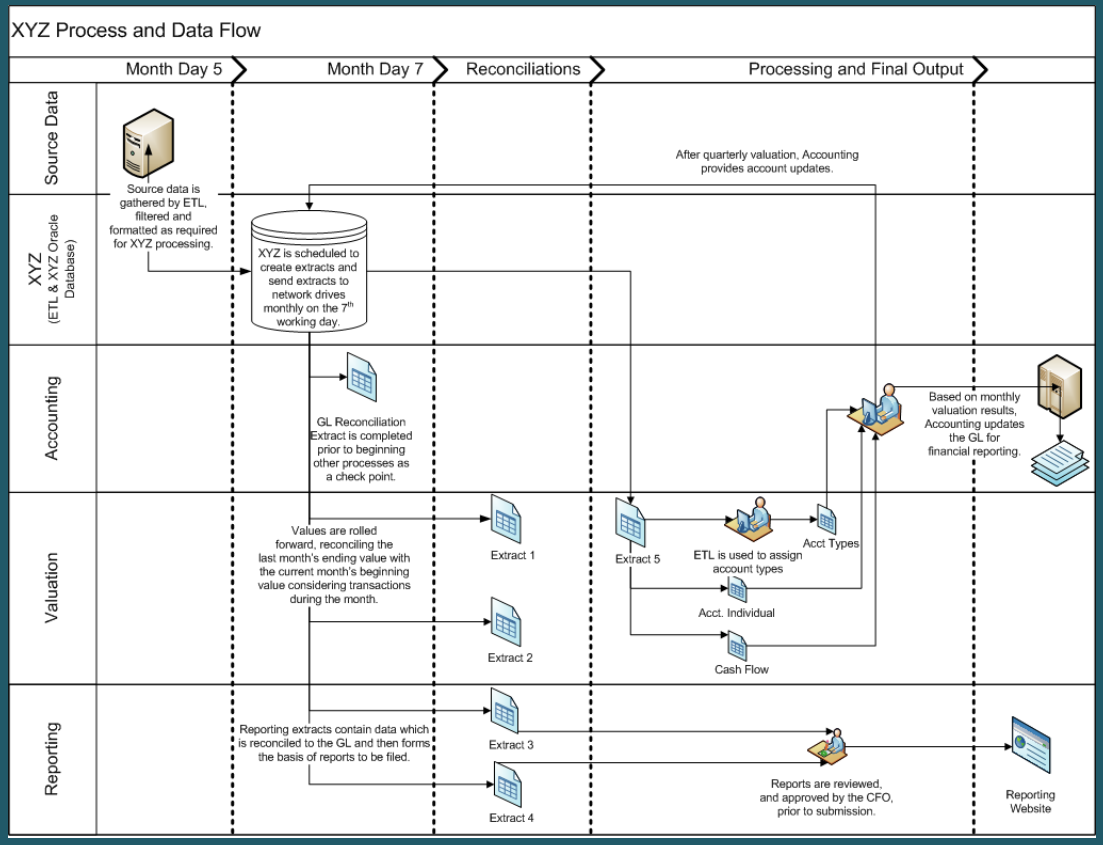
Technology Component	Component Description	Application Operating System	Database	Database Server	Database Operating System	Datacenter Location	In-House or Vendor Devloped	Vendor / Outsourcing	IT Owner	Business Owner	Access Administration Process	Change Control Process	Notes
XYZ	XYZ is an Oracle database used to consolidate and process data from source systems and files (sourced via ETL). Programming logic is contained in stored procedures, which are used with views to create extracts (Excel spreadsheet reports) used for Accounting and Reporting.	N/A	Oracle 11g	XYZPROD	UNIX - Solaris	Birmingham	Vendor Developed	N/A - System is maintained in-house.	John Q. Owner	Suzie Q. Owner	Security Administration - Accounts for Authentication via Active Directory and Database Administration - Access Privileges in Oracle	Distributed System Change Control Process	N/A
CRM	Customer Relationship Management system stores customer information including all accounts and relationship data such as interests and hobbies.	z/OS	DB2	N/A - mainframe	z/OS	Atlanta	Vendor Developed	Yes - Vendor provides support services and SAS 70 is available	John Q. Owner	Suzie Q. Owner	Security Administration	Security Administration	N/A

CONTROLS

- Custom-Built Systems
  - Use inquiry to discover
  - Are they properly documented?
- Vendor / “Off the Shelf” Systems
  - Use walkthrough to discover
  - Gain a general understanding
    - Especially first time an application is used
    - Need to establish a baseline understanding of controls and configuration for apps like SAP, Oracle, etc.
  - Determine vendor’s responsibility
    - Vendor management practices
    - Vendor monitoring

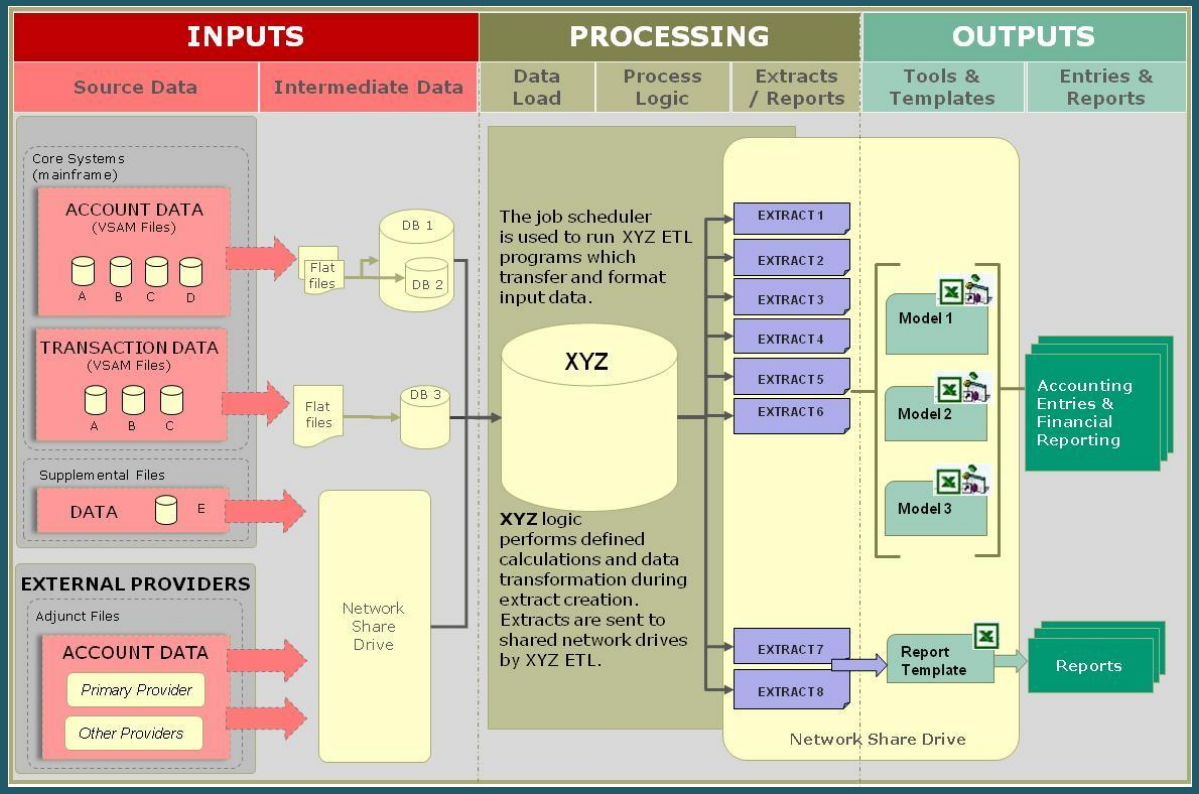
CONTROLS

Control evaluation requires understanding of the business process and data flow.



CONTROLS

Controls can be simply identified and categorized as input, processing, and output controls.



CONTROLS

- Application Input Controls:
  - Access security
  - Data validation
  - Coding controls
  - Input error correction
  - Batch controls (where applicable)

CONTROLS

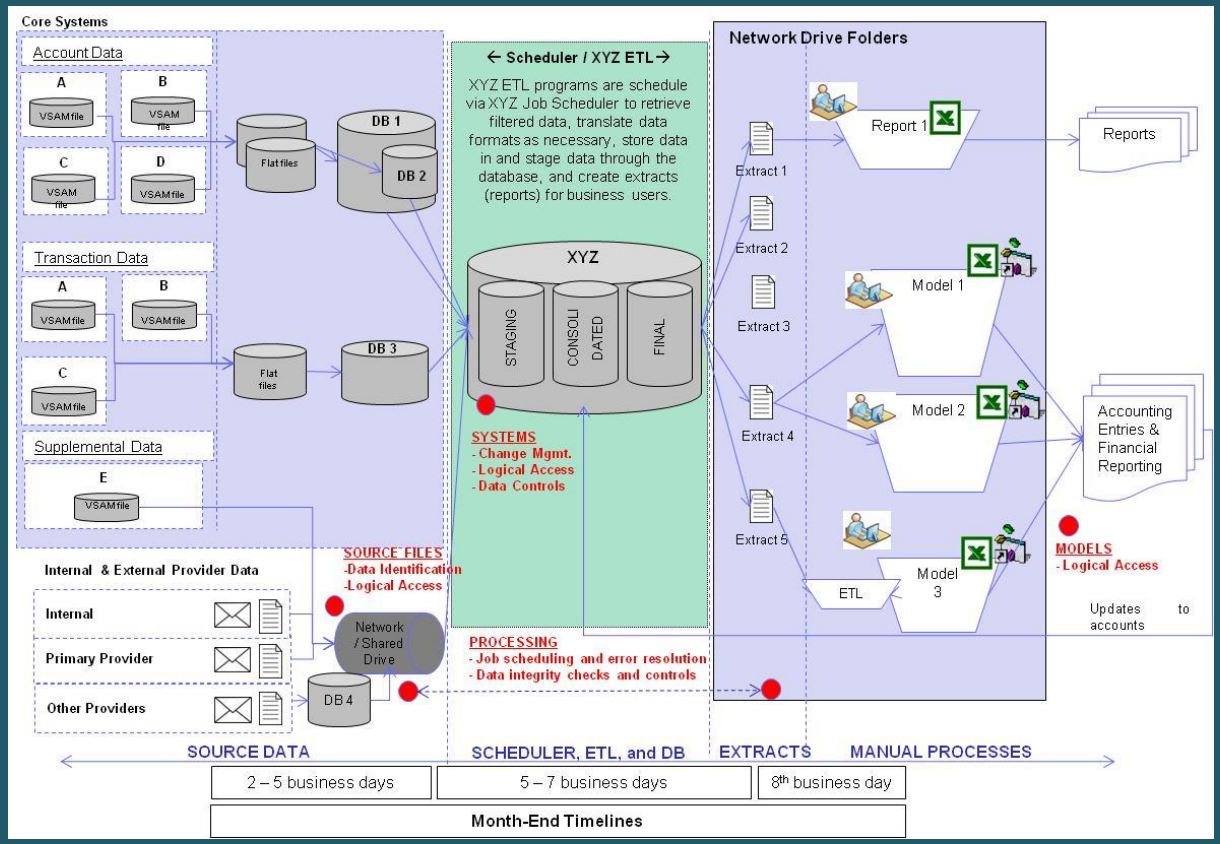
- Application Processing Controls
  - Level of automation (from fully manual to fully automated)
  - Job scheduler dependencies and monitoring
  - Auto calculations
  - Auto reconciliations
  - Auto notifications

CONTROLS

- Application Output Controls:
  - Reconciliations
  - Reviews
  - Approvals
  - Error reports/lists
  - Control over physical reports

CONTROLS

Analysis of defined risks, scope, and controls will point to areas of focus.



FUNCTIONALITY

- Verify functionality against requirements
- Verify end-user acceptance for newly installed
- Special considerations:
  - Security
  - Operational controls
  - Financial controls

FUNCTIONALITY

- What is the purpose of the application?
- What various scenarios should be considered to understand/test functionality?
  - For example: Use a broad scope of scenarios to test security
- Use system model in analysis and testing

TESTS

- Internal tests within the application
- Interface tests between systems
- Tests of data used by the application

COMPLICATIONS

- Proprietary Apps
  - Inherent risks
- Data Warehouse
  - Inherently prone to data errors due to nature of sourcing across the enterprise
  - Inherently needs strong change management controls due to the number of persons and systems complexity

COMPLICATIONS

- Data Warehouse
  - Data integrity
    - That is, processing did what it should have done, successfully
  - Data quality
    - Data entered and processed was valid, accurate, and complete

FINANCIAL ASSERTIONS

- Do application controls address the primary assertions of the account or cycle?
- Test the application against the specific financial assertion related to the account or cycle:
  - Accuracy
    - Data entry validation controls
    - Auto calculations
  - Existence
    - Application data entry validation controls
    - Database data value requirements
  - Completeness
    - Job/Batch processing controls
    - Reconciliations

TOOLS

- CAATs
  - Data mining
  - Data analysis

- ETL
  - Use to look for flawed data that is a result of a flawed application or process

TOOLS

- Examples:
  - Possible tests of controls
    - Reconciling (e.g., customer id in transaction file to master file)
    - Recalculating (e.g., extend inventory)
    - Duplicates (source documents, fraud, error)
    - Gaps (source documents, errors)
    - Benford's Law (fraud, statistical assurance)
  - Use CAAT to re-perform auto calculations and reconciliations

TOOLS

- Examples:
  - Data mining to support audit objectives
  - Code analysis --
    - Group codes to ensure data integrity (i.e., make sure a non-existing code wasn't entered in error and the app allowed it)
  - Purchase order threshold --
    - Proper authorization of purchases over a threshold
    - Match expenditures to purchase orders for amounts => than threshold
    - That is, app allows expenditures over P.O. threshold
  - Credit card threshold --
    - Classify expenses by vendor to see if threshold is being manipulated

TOOLS

- Examples:
  - Data mining to support audit objectives
  - Credit memos
    - Classify by rep to see if “normal distribution”, and proper authorization (person entering the C/M has authority to approve or key C/M) – app or interface exercising proper authorization controls
    - Stratify by amount for normal distribution (i.e. data integrity)
    - Benford’s Law, same purpose
  - Inventory anomalies --
    - Check receiving reports for negative amounts received
    - Check file maintenance changes to ensure inventory prices and quantity on hand is not being manipulated prior to physical counts)

REPORTING

- Usually self-evident
  - Audit objective
  - Tests conducted
  - Results
  - Recommendations

REFERENCES:

Guide to Audit of IT Applications:
http://www.isaca.ch/files/DO2_ISACA/thk_vorgehensmodell_e.pdf

Auditing Application Control – Oracle
http://www.auditnet.org/docs/Auditing_Application_Controls.pdf

The Application Audit Process
http://www.sans.org/reading_room/whitepapers/auditing/application-audit-process-guide-information-security-professionals_1534

ISACA Journal – 2012 volume 3
(Forthcoming)

Tommie Singleton, Ph.D., CISA, CGEIT

singleton_tommie@columbusstate.edu