FOX | ITACS

Master of IT Auditing & Cyber Security

IT Audit Process

Michael Romeu-Lugo MBA, CISA

March 6, 2015

Engagement Planning – Audit Plan (Definition)

1. A plan containing the nature, timing and extent of audit procedures to be performed by engagement team members in order to obtain sufficient appropriate audit evidence to form an opinion.

    a. the areas to be audited,
    b. type of work planned,
    c. high-level objectives and scope of the work, and topics such as
    d. budget, resource allocation,
    e. schedule dates, type of report and its intended audience, and
    f. other general aspects of the work

2. A high-level description of the audit work to be performed in a certain period of time.

Engagement Planning – Definitions

- **Audit Risk** - The risk of reaching an incorrect conclusion based upon audit findings.
    - **Control Risk** - Control risk is the risk that an error that could occur in an audit area and could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system.
    - **Detection Risk** - the risk that professionals' substantive procedures will not detect an error that could be material, individually or in combination with other errors.
    - **Inherent Risk** - Inherent risk is the susceptibility of an audit area to err in a way that could be material, individually or in combination with other errors, assuming that there were no related internal controls.

- **Materiality** - An audit concept regarding the importance of an item of information with regard to its impact or effect on the subject matter being audited. An expression of the relative significance or importance of a particular matter in the context of the engagement or the enterprise as a whole.

Engagement Planning - Definitions

- **Risk Assessment** - A process used to identify and evaluate risk and its potential effects.
  - Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan.
  - Risk assessments are also used to manage the project delivery and project benefit risk.

Performance Standard 1201 – Engagement Planning

1201.1 IS audit and assurance professionals shall plan each IS audit and assurance engagement to address:

- Objective(s), scope, timeline and deliverables
- Compliance with applicable laws and professional auditing standards
- Use of a risk-based approach, where appropriate
- Engagement-specific issues
- Documentation and reporting requirements

1201.2 IS audit and assurance professionals shall develop and document an IS audit or assurance engagement project plan, describing the:

- Engagement nature, objectives, timeline and resource requirements
- Timing and extent of audit procedures to complete the engagement

Audit Phases

Audit Phase	Description
Audit Subject	• Identify the area to be audited.
Audit Objectives	• Identify the purpose of the audit. For example, an objective might be to determine whether program source code changes occur in a well-defined and controlled environment.
Audit Scope	• Identify the specific systems, functions or unit of the organization to be included in the review. For example, in the previous program changes example, the scope statement might limit the review to a single application system or to a limited period of time.
Pre-audit Planning	• Identify technical skills and resources needed. • Identify the sources of information for test or review of such functional flow charts, policies, standards, procedures and prior audit work papers. • Identify locations or facilities to be audited. • Develop a communication plan at the beginning of each engagement that describes who to communicate to, when, how often and for what purpose(s).

CoreTech, Inc. Internal Audit Assurance Program

Data Backup and Restore Procedure

Objectives:

- **Control Objective(s):**
  - IT Personnel perform daily backups on CTI data. After backups are completed, IT personnel review backup status to confirm successful completion.
  - Restores from backup media will work when required.

- **Assurance Objective(s):**
  - Verify CTI's compliance with existing data backup and restoration procedures.
  - Ensure data backups are performed according to an established schedule
  - Verify that backups are tested on a regular basis as defined by standard operating procedures
  - Verify that problems (issues) are addressed in a timely manner avoiding any impact on production

CoreTech, Inc. Internal Audit Assurance Program

Data Backup and Restore Procedure

Scope

- The review will focus on the regular execution of backup and restore procedures during the period of July 1, 2014 through September 30, 2014 (third quarter, 2014). This includes the review of established procedures and relevant documentation.
- Review of backup media storage and overall management are not within the scope of this review.

Pre-audit Planning

- **Technical Skill(s):** N/A
- **Resource(s):** SAP System Administrator, IT Operations Manager
- **Documentation:**
  - Current version of backup and restore procedures
  - Backup and restore log(s) for the period in review
  - Job descriptions – SAP System Administrator, IT Operations Manager
- **Location(s):** Philadelphia Data Center

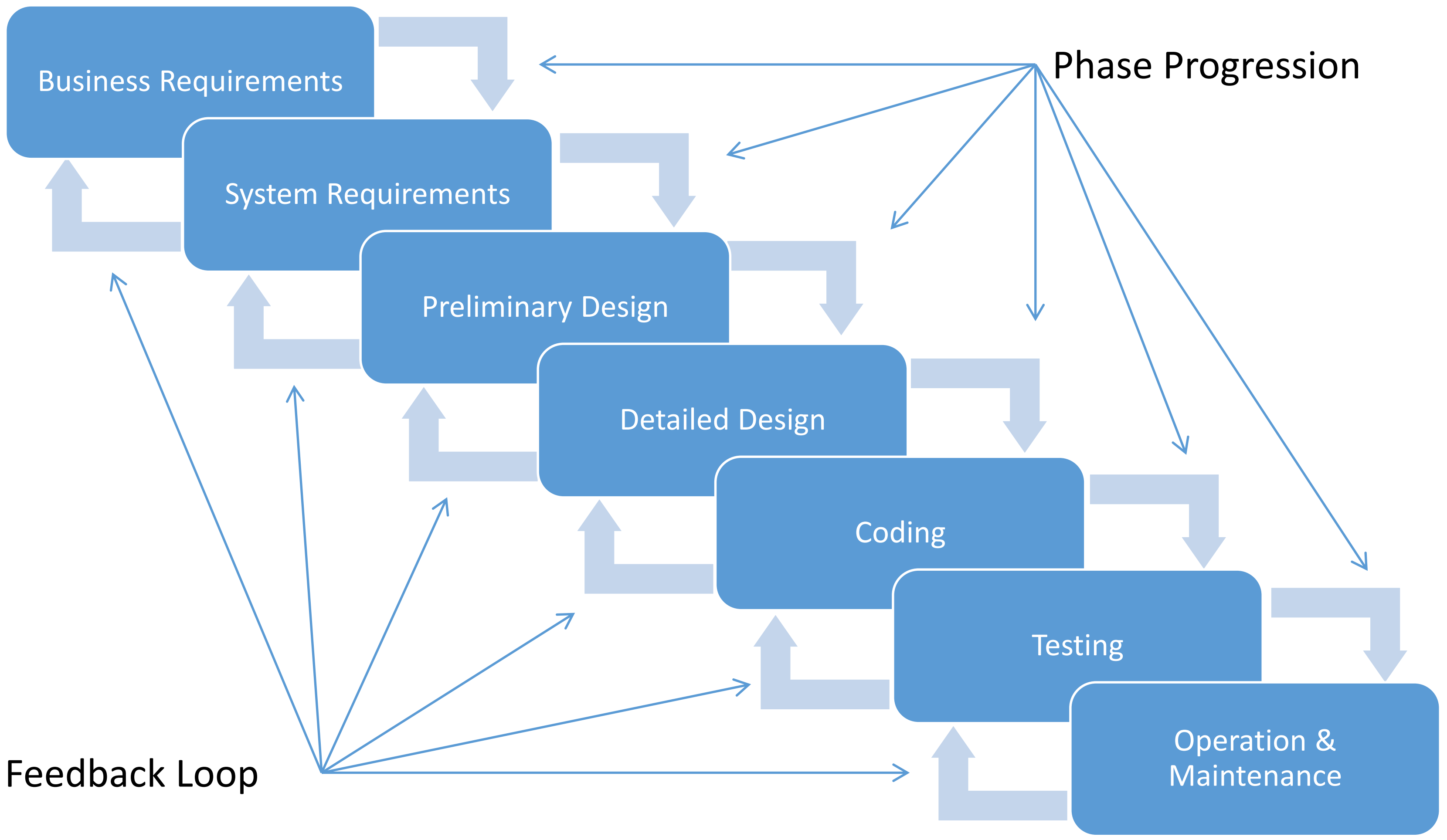
Audit Phases

Audit Phase	Description
Audit procedures and steps for data gathering	• Identify and select the audit approach to verify and test the controls. • Identify a list of individuals to interview. • Identify and obtain departmental policies, standards and guidelines for review. • Develop audit tools and methodology to test and verify control
Procedures for evaluating the test or review results	• Identify methods (including tools) to perform the evaluation. • Identify criteria for evaluating the test (similar to a test script for the auditor to use in conducting the evaluation). • Identify means and resources to confirm the evaluation was accurate (and repeatable, if applicable).
Procedures for communication with management	• Determine frequency of communication • Prepare documentation for final report
Audit report preparation	• Disclose follow-up review procedures. • Disclose procedures to evaluate/test operational efficiency and effectiveness • Disclose procedures to test controls. • Review and evaluate the soundness of documents, policies and procedures.

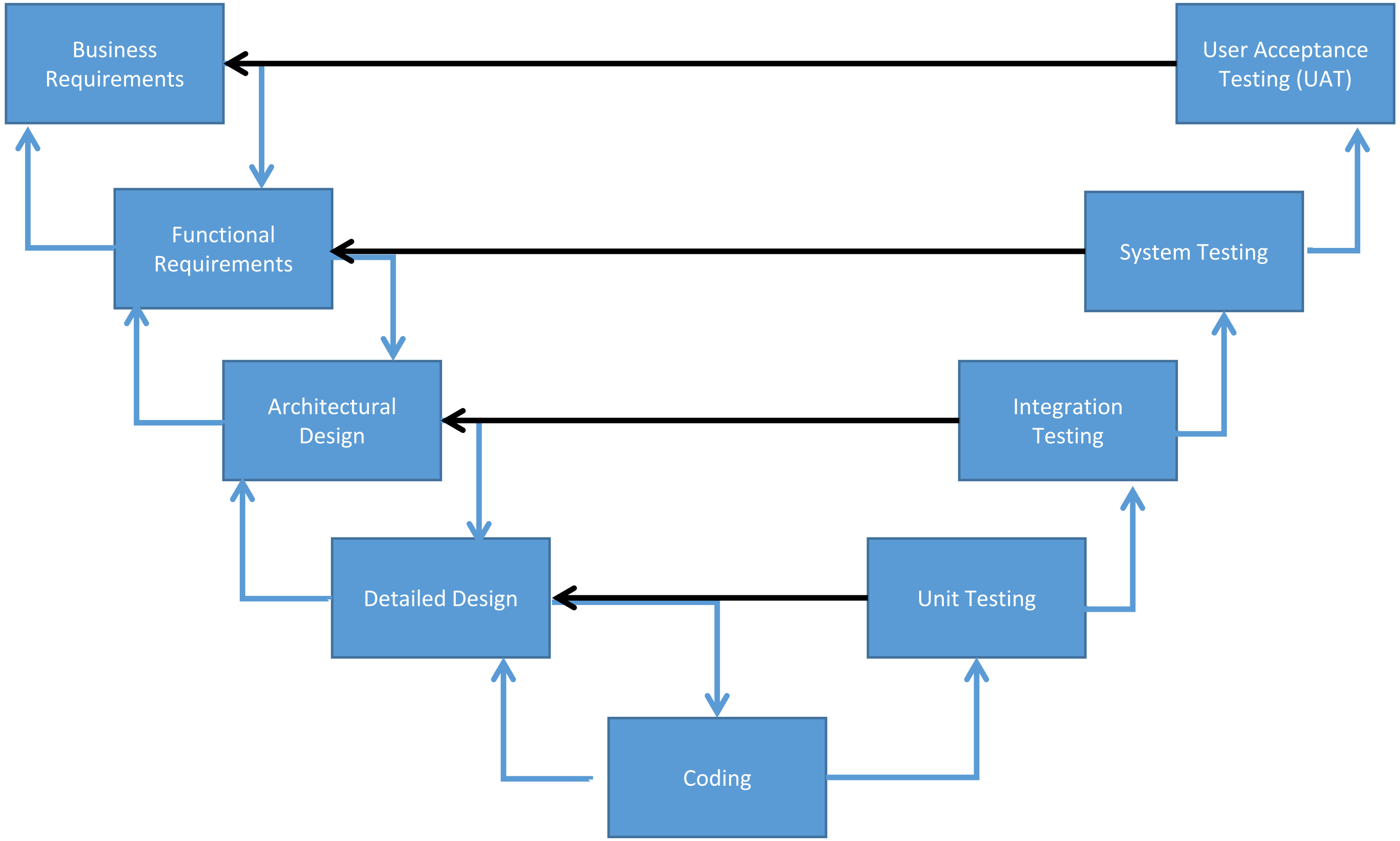
Classification of Audits

Compliance Audit	• Verify compliance with laws, regulations and contracts.
Financial Audit	• Verify the accuracy of financial reports
Operational Audit	• Review internal controls structure of a process area
Integrated Audit	• Financial Audit + Operational Audit
Administrative Audit	• Operational productivity
IS Audit	• Safeguard IT Assets, CIA, Risk Management
Forensic Audit	• Discovery and disclosure of crime
Specialized Audit	• Third-party audit

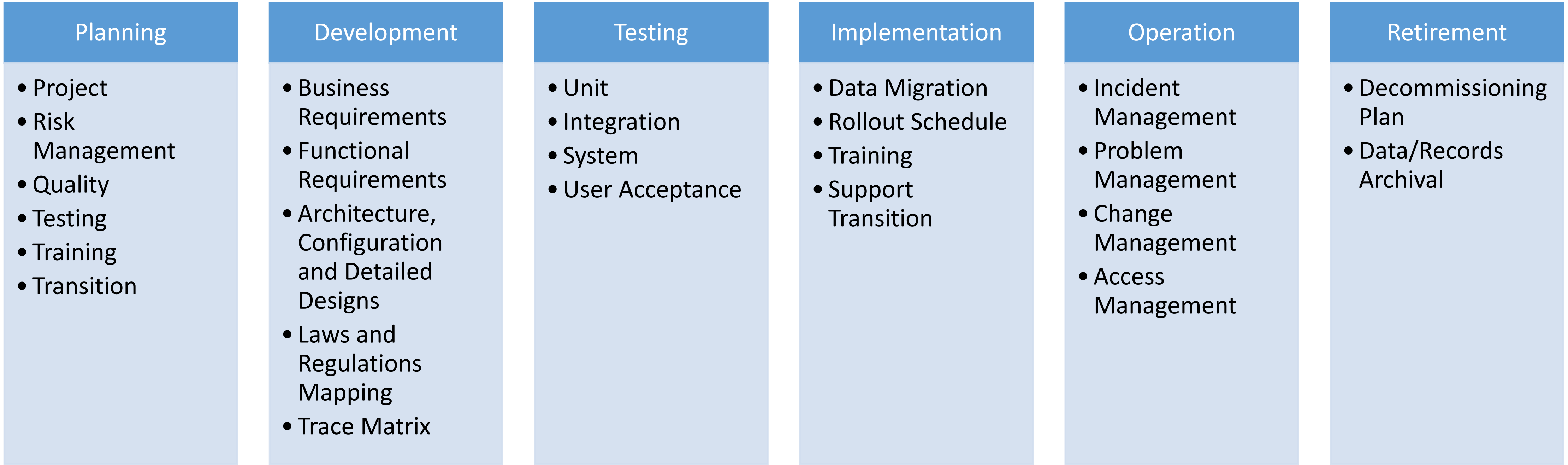
Boehm’s Waterfall Model



Verification and Validation or V-Model



SDLC Life Cycle Controls – Activities and Documentation



Planning

- Project
- Risk Management
- Quality
- Testing
- Training
- Transition

Development

- Business Requirements
- Functional Requirements
- Architecture, Configuration and Detailed Designs
- Laws and Regulations Mapping
- Trace Matrix

Testing

- Unit
- Integration
- System
- User Acceptance

Implementation

- Data Migration
- Rollout Schedule
- Training
- Support Transition

Operation

- Incident Management
- Problem Management
- Change Management
- Access Management

Retirement

- Decommissioning Plan
- Data/Records Archival

Risk Assessment – Enterprise Software in MedDev Industry

Risk Category	Description
Regulatory Risk	• Good Manufacturing Practices • Good Clinical Practices • Good Laboratory Practices
Safety Risks	• Patient Safety • Personnel Safety • Product Quality
Compliance Risks	• Quality System Regulations • Electronic Signatures and Records • Internal Policies and Procedures
Technology Risks	• Functional Risks • Industry Maturity
Software Category (Complexity)	• Category 1 – Infrastructure Software • Category 3 – Non-Configurable Software • Category 4 – Configurable Software • Category 5 – Custom Software

Software Examples

Minitab® is a leading statistical analysis software package. It is mainly used for statistics-based process improvement. Engineers use the software to evaluate process variability and identify opportunities for improvement… Six Sigma.

ETS is an eLearning software used to manage employee training. The software is used exclusively in the Manufacturing Operations division. ETS includes modules for Scheduling, Training Delivery and Evaluation, and Reporting. ETS was launched in 2008 by ETS, Inc. to address a major gap in eLearning software for the Food Industry.

CalTrack was developed by C. Smith in 2004. Mr. Smith is an Associate Maintenance Engineer working at the Darby, PA manufacturing development facility. Processes are designed or improved at this facility then implemented in the US manufacturing facilities once they have been successfully tested. CalTrack is an MS Access ® based application that tracks equipment calibration. Engineers record calibration data into CalTrack which then tracks calibration status for the equipment.

Classification of Audits

- **Compliance Audits** – Test adherence to regulations or industry standards

Goal	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all Access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Classification of Audits

- **Financial Audits** – To assess the accuracy of financial reporting
  - Concern: integrity and reliability of information (which controls?)
- **Operational Audits** – evaluate the control structure of a particular process or area.
  - Examples: System and logical controls
- **Integrated Audits** – Financial + Operational Audits
- **Administrative Audit** – evaluate the efficiency and operational productivity within an organization.
  - Examples: Change and Incident management
- **IS Audit**
  - Information Asset Safeguards
  - CIA
  - Relevant and reliable information
  - Prevent, detect and correct risks

Classification of Audits

- **Forensic Audits** – Specialized in discovering, disclosing and following up on fraud and crimes.
  - Chain of Custody – the chronological documentation or, showing the seizure, custody, control, transfer, analysis and disposition of physical or electronic evidence.
  - Evidence preservation is key!
- **Specialized Audits** – SSAE 16
  - Type 1 – "a report on management's description of a service organization's system and the suitability of the design of controls."
  - Type 2 – Type 1 + Auditor's description of the system and the suitability of the design of controls.

Forensic Audits

“The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise.” (Forensic Examination).

- Activities
  - eDiscovery – Identification, Preservation (legal hold), Collection, Processing, Review, Production. What constitutes a Record?
  - Recovery and Reconstruction
  - Forensic Analysis
- Chain of Custody – Validity and Integrity of Data.
  - Who had access to the data when
  - Is it the exact item that was recovered or tested

Challenges in Forensic Computing

- Linking illegal activity to person(s)
  - Threatening e-mail case
- Establishing intent
  - Pharmalink Case
- Expertise
  - Deep technical knowledge
  - Qualifications and Experience
  - Independence and Objectivity – The use of outside counsel and expertise to preserve independence and objectivity

Specialized Audits

- Audit and analysis procedures focusing on specific items or processes selected by the client.
- Generally address compliance with regulations and contractual agreements.
- Examples
  - SOX Audits (SEC) – general accounting and financial controls
  - HIPAA Audits (HHS) – compliance with Privacy, Security and Breach Notification rules. Both Covered Entity And Business Associate.
  - QSR (FDA) / ISO 13485 (International) – Quality System Regulations for Medical Devices
  - Software Licensing Audits
  - Contract Audits

Audit Programs and Methodologies

"A step-by-step set of audit procedures and instructions that should be performed to complete an audit."

- Scope of the audit
- Audit Objectives
- Audit procedures
- Evidence gathering process to support audit conclusions and opinions
  - Sufficient
  - Relevant
  - Reliable