FOX | ITACS
Master of IT Auditing & Cyber Security

IT Audit Process

Michael Romeu-Lugo MBA, CISA

March 27, 2017

Agenda

- Audit Planning
  - PS 1203 / PG 2203
- Evidence
  - PS 1205 / PG 2205
- References:
  - ITAF 3rd Edition
  - Information Systems Auditing: Tools and Techniques – Creating Audit Programs

Performance Standard 1203 – Performance and Supervision

ITAF 3rd Edition, page 10

Statements - "IS audit and assurance professionals shall…"	
1203.1	Conduct the work in accordance with the approved IS audit plan to cover identified risk and within the agreed-on schedule.
1203.2	Provide supervision to IS audit staff for whom they have supervisory responsibility, to accomplish audit objectives and meet applicable professional audit standards.
1203.3	Accept only tasks that are within their knowledge and skills or for which they have a reasonable expectation of either acquiring the skills during the engagement or achieving the task under supervision.
1203.4	Obtain sufficient and appropriate evidence to achieve the audit objectives. The audit findings and conclusions shall be supported by appropriate analysis and interpretation of this evidence.
1203.5	Document the audit process, describing the audit work and the audit evidence that supports findings and conclusions.
1203.6	Identify and conclude on findings.

Performance Guideline 2203 – Performance and Supervision

ITAF 3rd Edition, Page 95

- **Planning and risk assessment**
  - 1201 Engagement Planning
  - 1202 Risk Assessment in Planning
- **Identifying controls**
- **Assessing controls and gathering evidence**
  - Design effectiveness
  - Operational effectiveness
- **Documenting work performed and identifying findings**
- **Confirming findings and following up on corrective actions**
  - Confirm with Auditee
  - If corrected before end of engagement auditor should mention original findings and document actions taken
- **Drawing conclusions and reporting**
  - 1204 Reporting
  - Draw conclusions and report about impact of finding on audit objectives

Performance Guideline 2203 – Performance and Supervision

ITAF 3rd Edition, Page 98

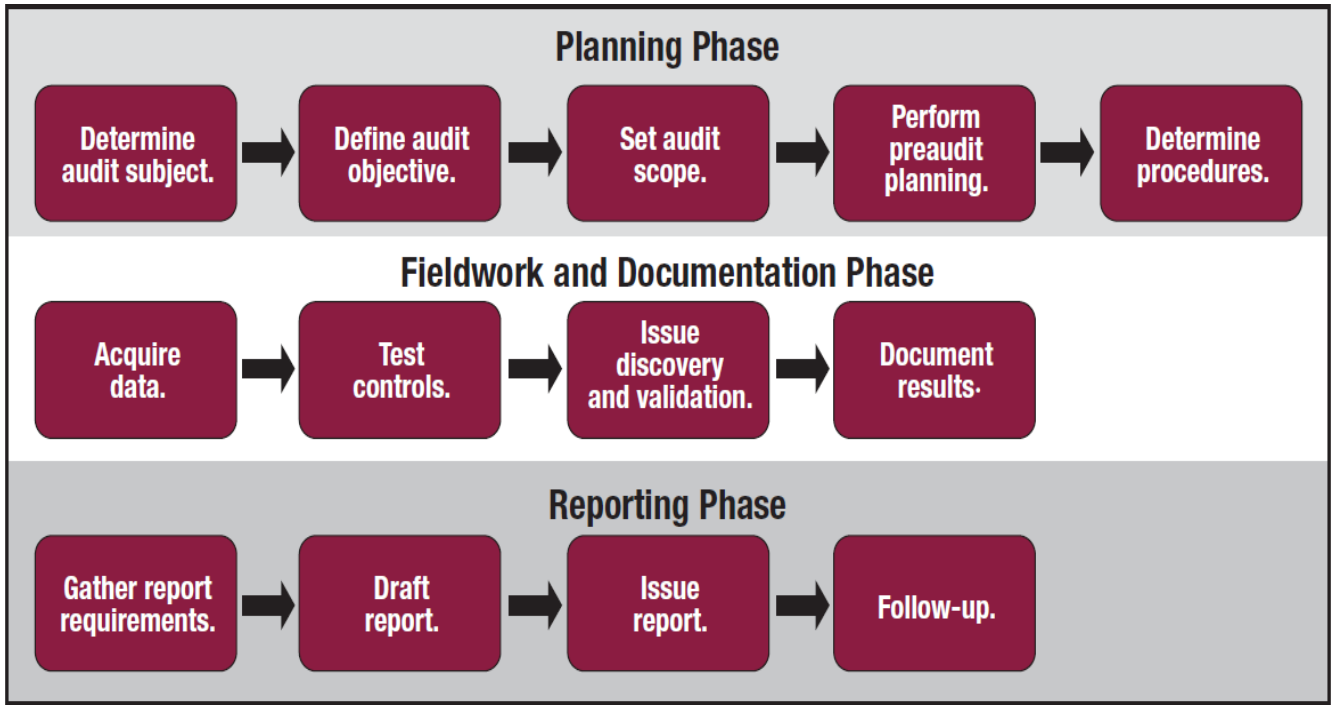
Documenting

Professionals should prepare sufficient, appropriate and relevant documentation in a timely manner that provides a basis for the conclusion and contains evidence of the review performed. Sufficient, appropriate and relevant documentation should enable a prudent and informed person, with no previous connection to the audit engagement, to re-perform the tasks performed during the audit engagement and reach the same conclusion. Documentation should include:

- Audit engagement objectives and scope of work
- Audit engagement project plan
- Audit work programme
- Audit steps performed
- Evidence gathered
- Conclusions and recommendations

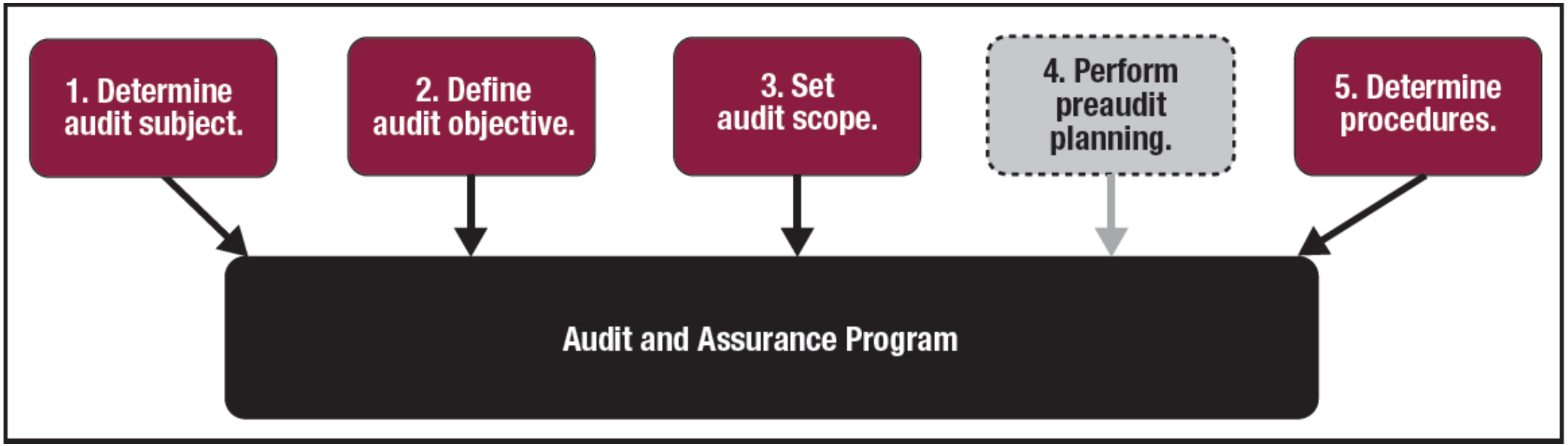
Audit Work Programme*

- "Work Programme" = "Audit Program"
- Procedures and instructions
  - Test controls
  - Evaluate results
  - Obtain suitable evidence to form an opinion
  - Report findings to stakeholders
- Include:
  - Areas to be audited
  - High-level objectives
  - Tools and techniques for testing controls



* Information Systems Auditing: Tools and Techniques – Creating Audit Programs

Audit Program – Planning Phase



Audit Program – Planning

Steps	Examples	Sources of information
1. Define audit subject	• ERP system • Data Center • BYOD Security	• Annual audit plan • Risk assessment • Organizational change plans • Legal / regulatory changes • Mergers and Acquisitions
2. Define audit objective	• ERP Inventory management • DC environmental controls • iOS devices	• Annual audit plan • Audit management • Executive management • Previous audit reports • Internal policies, standards and procedures • Risk assessments • Legislation or regulations applicable to enterprise.
3. Set audit scope	• Assuring compliance with SOX • SAP MM – Inventory Management • Data Center Temperature and Humidity Controls • iOS data protection and encryption	• Legislation or regulations applicable to enterprise • Previous audit results • SLA and compliance issues • Problem and Incident tickets

Audit Program – Planning (continued)

Steps	Examples	Sources of information
4. Perform preaudit planning	• Location of IT functions supporting SAP MM, location of supply operations personnel. • Philadelphia Distribution Center: 2017 Broad Street, Philadelphia PA • Mobile Management organization	• Organization charts • Previous audit reports • Process maps and flow diagrams • Vendor contracts • Network maps

Audit Program – Planning: Step 5 Develop Procedure

Activity	Example
• Identify and obtain departmental policies, standards and guidelines for review	• Information security policies • Segregation of duties (SoD) policies • Purchasing policies • Authorization matrix • Industry standards or guidelines • Compliance requirements
• Identify a list of individuals to interview	• Accounts payable clerks • Subject matter experts (SME) • Supervisors and Managers

• Identify methods (including tools) to perform the evaluation.	• Compliance Testing
	• Substantive Testing
	• Tools
	  • Questionnaires
	  • Checklists
	  • Spreadsheets
	  • Computer Assisted Auditing Tools (CAATs)

Audit Program – Planning: Step 5 Develop Procedure

Activity	
• Develop tools and methodology to test and verify controls.	• See the previous step: "Identify methods (including tools)…"
• Identify criteria for evaluating the tests (similar to a test script for the auditor to use in conducting the evaluation).	• Organization Structure Review • Policies, standards and procedures review • Documentation review (user manuals, training material, …) • Interviews with key personnel • Observation of procedures as they are performed • Reperformance • Walk-Throughs • Data analysis
• Define a methodology to evaluate that the testing and its results are accurate (and repeatable if necessary).	• Refer to standard 1205 – Evidence

Performance Standard 1205 - Evidence

Statements
1205.1 IS audit and assurance professionals shall obtain sufficient and appropriate evidence to draw reasonable conclusions on which to base the engagement results.
1205.2 IS audit and assurance professionals shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

Evidence must be:

- **Relevant** – consistent with audit objectives and supports audit findings and recommendations.
- **Reliable** – accurate, verifiable and from objective sources.
- **Sufficient** – factual, adequate and convincing such that a prudent person would reach the same conclusions as the auditor.

Evidence-Gathering Procedures

Procedure	Comments
Inquiry and Confirmation	• Least reliable. Consists of interviews usually driven by checklists.
Inspection of Records	• Paper, computer printouts, plans and reports, etc. Originals are better than copies; system-generated; gathered by auditor.
Inspection of Assets	• Existence and condition. Verify/record ID, serial#, etc.
Observation	• Watching a person or system execute the process or transaction
Re-performance	• Executing again and recording how it happens, not how it should happen.
Re-calculation	• Carrying out calculations manually or by other independent means recording the results.
Scanning	• Looking for things that do not belong or do not follow a pattern.

Other Evidence Considerations

- Source, nature and authenticity
  - Written rather than oral
  - From independent sources
  - Obtained professionally rather than by auditee
  - Certified
  - Kept by an independent party
  - The results of inspection and observation
- Identify, cross-reference and catalogue
- Retention, availability and disposal
- Protect from unauthorized disclosure or modification

Coming Soon – Next Week

- Sampling
  - Sampling Types
  - Sampling Techniques

- Testing Techniques