How to survive an Audit

Eric Tan
PwC

Harshul Joshi
PwC

Objectives

- • Preparation - You can never prepare enough;
- • Mock audit - Running a mock audit
- • Documentation to prove the processes and controls - Documentation is king
- • Is email documentation?
- • How much information to volunteer? - Respond to the point
- • More is more?
- • Liaison between your internal technical folks and the auditor
- • Developing a internal quality program - Peer reviews
- • Collaborating with your external auditors
- • Believe it or not, everybody wants to do the right thing?
- • The devil is in the details - Know when to get the right experts involved.
- • Ensuring objectives and scope are clearly defined.

Type of Audits

- External Audit (SOX requirements)
- Internal Audit
- Compliance and Regulatory based audits (PCI, SOX, FISMA, Vendor based)
- Technical Assessments (Configuration reviews, Server hardening)

So what's the point?

- Resource mapping before execution
- Having the right resources available for the auditors
- Having the right context and scope
- Methodologies and Tools

Scoping

- Technology Areas

Case Study - PCI

- What are the requirements
- Preparation
- Going through the audit
- Findings
- Sustaining PCI

Case Study – ISO 27001 / 2

- What are the requirements
- Preparation
- Going through the audit
- Findings
- Sustaining

Backing up the procedures

- How to produce auditable proof?
- What is a auditable process?

Ensure Sufficient Planning

- Ensure that scope and objectives are clearly define – Avoid scope creep.
- Schedule and allow time for sufficient involvement, feedback, input and audit team leader and manager
- Budget sufficient time for execution of audit, allowing time to:
  - Prepare to research and to design tailored questions
  - Plan the meeting to allow sufficient time so that the meeting is not rushed
  - Document findings as soon as possible after the meeting
  - Debrief and plan to corroborate findings and/or perform additional testing
- Ensure timing with client contacts considering their busy season is likely not yours

Basic Ground Rules for Meetings

- Ensure meetings are prepared well ahead of time; agenda, meeting objectives, specific detailed questions you want to ask.
- Learn to always apply professional skepticism and, whenever possible, support the explanations given to us by asking the our ‘clients’ to show us reports and procedure manuals or other documents used in, or generated by, the performance of the controls.
- Team composition is critical. Don’t go at it on your own. Spread responsibility over the team (e.g. security, ERP, data management). Where appropriate, involve technical specialist involving them as needed during planning, execution and delivering results
- Document timely, clearly and concisely.

Always Be On The Alert

- Healthy skepticism means that we do not necessarily assume the honesty of management
- Be alert to fraud risk indicators and perform specific required fraud inquiries, as necessary
- Do not rely solely on management representations - corroborate them or use observation, examination and reperformance of evidence of the control so that we do not simply audit by conversation
- Recognize conflicting information (e.g., contradictory representations from different entity personnel or information that is inconsistent with our own views based on our analytical procedures)

Learn to Ask Probing Questions

- We should ensure that our inquiries of management are sufficiently detailed. For example, asking a security manager if he reviews a security violation report is insufficient. We need to validate that the control is effective by evaluating corrective actions taken. In this example, appropriate questions might include the following:
  - How is the report reviewed? Is every report reviewed? How long does the review take? How are the items investigated?
  - Are there particular situations to which the manager's attention is directed?
  - Is there a record of the investigation and results?
  - Are those problems being eliminated? Are the resolutions documented?
  - What do you do when you find an error or what are you looking?
  - What kinds of errors have been found? What happened as a result of finding the errors?
  - Are the reports ever not produced, or do reports ever have no entries on them?
  - Has anything ever occurred to suggest the report is not reliable?

Discussing and Presenting Issues

- Determine where to have your discussions. For example closing meetings vs. during field work.
- Carefully consider participants in your closing discussions (e.g. executive or managers) are present
- Determine method of delivery of observations – e.g. sharing ahead of time vs. working through the details together.
- Take into account the behavior of the individual and culture of the client.
- Consider if this is the first time the individual is undergoing and audit? How is he / she measured on the results?
- Consider the size and complexity of the client and systems.

Having Successful Meetings

- Effective interviewing technique includes using open, closed and probing questions, and avoids jargon
- Generally aim to keep to the agreed time; if you need more time, arrange a new appointment with the client immediately
- It is important to direct the meeting to avoid unnecessary topics and prevent wasted time
- Keep focused on what evidence you expect to get (relating to the "show me" meeting agenda)
- Do not leave follow-up and verification to another meeting
- Summarize at the end of the meeting to confirm your understanding

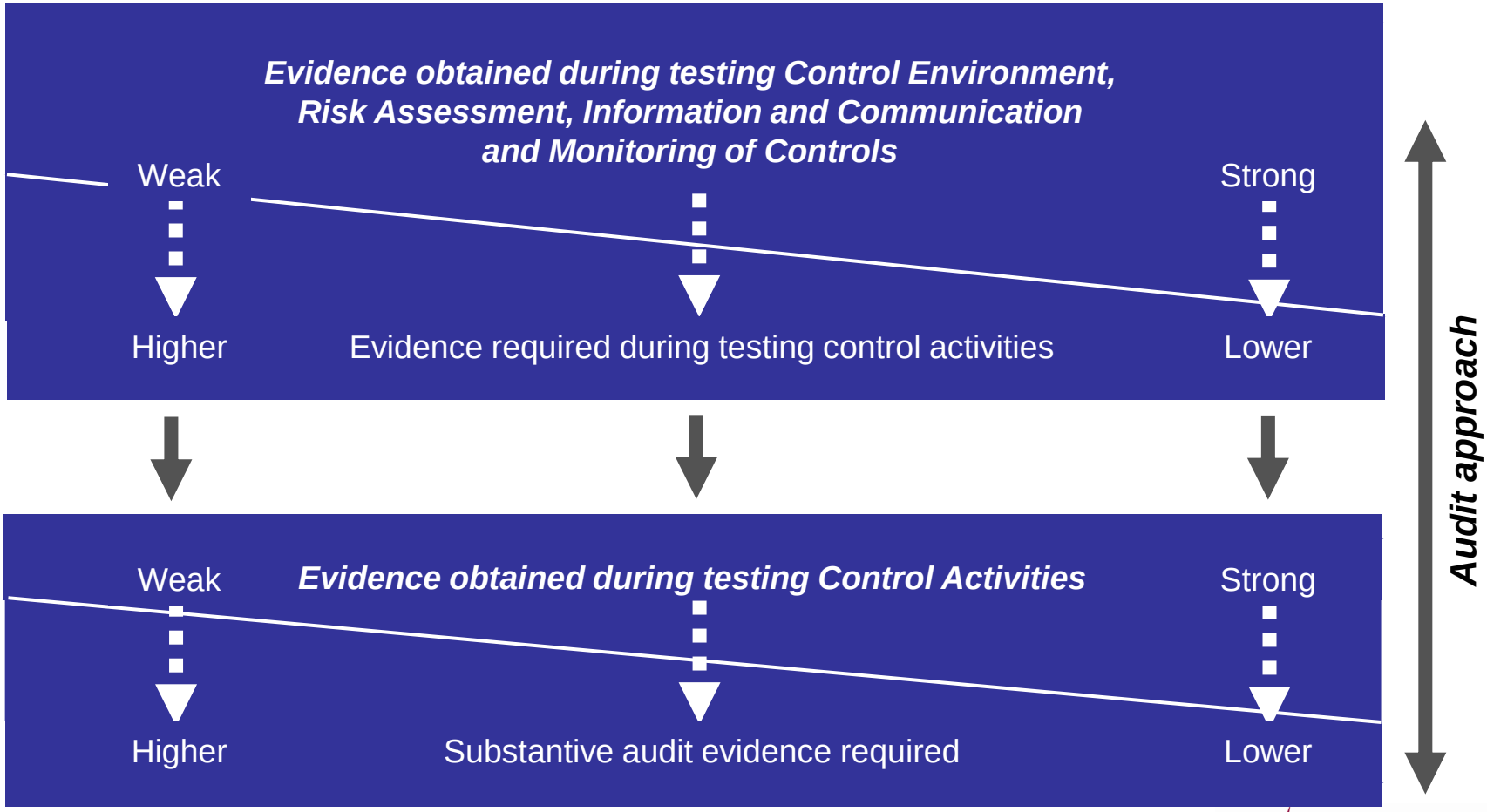
Documentation Considerations

- Ensure sufficient ‘footprint’ of team leader’s review in the audit
- Audit risks, focus areas and related controls
- Nature, timing and extent of testing performed (and thus whether we need to perform further testing)
- Consider whether we have recorded sufficient information where an independent reviewer can follow the thought process taken for the audit.
- Avoid delegating note-taking responsibilities to junior staff without giving them sufficient briefing beforehand
- Do not attempting to write up everything that was discussed during the meeting

Case Study – 404 Sarbanes Oxley

- Have all systems supporting financially significant process been identified?
- Have reports supporting both internal controls and financial statements been identified, tested for completeness and accuracy?
- How much test testing do we really need to do when an exception or error is found?
- Have we considered mitigating controls?

Internal Controls – The relationship with the Audit Approach



Case Study – System Implementation Assessments

- $300m implementation of supermarket system. Have all areas in scope been identified and risk ranked?
- Ensuring continuous ‘buy-in’ from various stakeholders is critical to the success of an audit.
- Have we validated inquiry procedures with evidence of execution controls?
- What is the basis of our assessment? Work-program? Framework utilized?

Final Consideration – Critical Self Review

- Have all procedures in the step been addressed?
- Were the audit objectives of the planned and executed procedures achieved?
- If exceptions were noted during testing, has an appropriate management letter comment been provided?
- Has consideration been given to how findings in a particular area impact the company?
- Are there any issues or questions that need to be discussed with a more senior team member immediately?