A Audit Process

A.1 Introduction

Like taught in the excellent course AUD507 (*Auditing & Monitoring Networks, Perimeters, and Systems*) of the SANS Institute, an audit is a small product, a business object whose purpose is to report on risks in an exploitable way for the management. It can be *described as the function of measuring something against a standard*. It leads to recommendations and remediations in order to fill the security gaps.

An IT audit can be performed at multiple levels whose policy, procedure and systems. It can scale to an entire organization environment or be limited to a subset. The first problem arises when the scope must be defined. One can then rely on a simple philosophy that forms the foundation of how the audit should be conducted as expressed in the following epigraph. This implies that an audit is something that must be incremented to cover more and more assets.

"Start small, then grow your scope."

JAMES TARALA, SANS Instructor

A.2 Terminology

There are some terms to be kept in mind when talking about audit. The term **Audit** itself was already introduced but another important related term is **Assessment**. It refers to a practical activity aimed to find gaps in the security of a system. One can thus see an audit as a set of assessments, matching assessment controls against a standard.

The **Scope**, as already introduced, refers to the *What* and must be defined without trying to cover everything at first sight. In order to complete this definition, **Targets** are identified and **Objectives** are described, answering the *Why* about the related assets.

But in practice, how can this scope be defined ? At this point, one still needs a methodology in order to target the right assets and objectives. One can then, for example, use a **Risk Driven** approach, that is, try to identify where the biggest risks are and then derive the famous assets and objectives. Once done, **Controls** can be selected, that is, the means to assess the assets regarding the objectives.

Once the audit is achieved, a **Report** gathering findings, recommendations and remediations can then submitted to the management for handling.

A.3 Process Overview

An audit can be structured in a systematic way through a common process, a course of action that favours its success. In the literature, several forms of this process exist. The one presented here is mostly inspired from the process presented in the book *Auditing Information Systems: Enhancing Performance of the Enterprise* (2015), written by Abraham Nyirongo.

Figure A.1: Generic IT system Audit Process

In this figure, one can point out that the audit process is essentially a matter of :

1. **Preparation**
   (Audit Planning & IT Environment)
2. **Execution**
   (Audit Execution & Testing and evaluation)
3. **Reporting**
   (Finding and Reporting & Follow-Up)

A.3.1 Audit Planning

The process starts with establishing a plan of the activities that will be conducted during the audit. Such a planning implies project management skills can then be supported by multiple existing tools. Creating a Gantt chart is certainly a good approach to achieve this phase, stating activities but also milestones, feedbacks, (either internal or external) meetings and so forth. Anyway, meetings with the client must be foreseen to discuss the expectations and deliverables, e.g. the engagement letter (stating the borders of what can be touched by the auditors in the client organization's environment).

A sample open-source tool to workout this phase could be GanttProject (a *free desktop project management app*).

A.3.2 IT Environment

This is where the scope is defined. This addresses the research of information about the environment of the audited organization such that the auditor has a correct understanding in order to determine appropriate audit objectives, controls, checklists and questionnaires to be applied, policies and standards to be checked against and also stakeholders into the audited organization. This leads to an audit schedule and generally ends by a meeting with the personnel from the organization to explain how the audit will be conducted.

Useful standards and guidelines are, for example, ISO27000 series, NIST SP series and especially SP 800-53 and SP 800-115. Checklists can also be found on cisecurity.org in the security benchmarks.

A.3.3 Audit Execution

This phase starts after the green-for-go from the organization following the definition of the scope (formalized in a deliverable and discussed through a meeting with the client), leading to a series of examinations according to the defined targets and objectives with the checklists and questionnaires. This phase mostly aims to answer questions related to the relevance of internal policies and procedures.

This phase should be supported by a database management system (e.g. MySQL server) in order to collect findings.

A.3.4 Testing and Evaluation

Then comes the practical assessment through hands-on testing on the systems in the client environment. This also relies on checklists and questionnaires but more from an operational point of view. During this phase, auditors search for evidence that the controls are correctly implemented and work as expected. This can lead to what is called audit exceptions when controls fail to meet the expectations.

The same database management system as for the previous phase can be used to gather findings. Regarding the methods and techniques, the NIST SP 800-115 provides a good practical guidance for testing, examination and interviewing.

A.3.5 Finding and Reporting

This is a tedious phase as it requires to analyze all findings, observations and evidences collected during the execution. The challenge is to make a report that explains findings in an understandable way for the management, but also providing recommendations and, if relevant, remediations to mitigate the risks at a technical level. This implies using management tools like scoring of vulnerabilities to facilitate the understanding of the risks. This generally leads to a presentation meeting with high executives from the management of the client organization.

A.3.6 Follow-Up

This phase can occur or not, directly after the audit or on agreed dates with the client organization. This aims to check if the recommendations were followed and, if not, why it fails to be applied. Through this, an auditor can identify if some problems eventually become recurrent.