A Process for Information Security Audits

By Thomas M. Smith, CD, CISSP

November, 2017

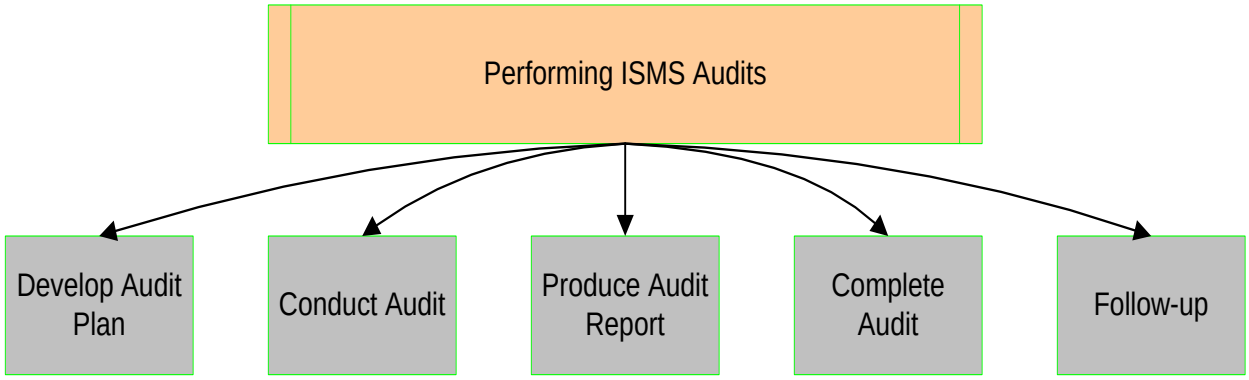
ABSTRACT

Whether an organization is adhering to the International Standard for an Information Security Management System (ISMS) or other requirements, it is usually necessary to conduct internal security centric audits. These audits do not necessarily follow the same rigour or practices that may apply to say a financial audit. Nonetheless, basic audit processes should be adopted and definitely adhered to as a minimum for any internal audit.

This paper outlines a process that can be implemented and is ideally suited for those who are implementing the ISO 27001 standard and required to conduct internal security audits. It provides all of the necessary components that can be applied to produce a needed audit report.

Process Overview

The following diagram depicts a process model that can be further developed to perform the security audit:



Each of these process activities is further explained below. Preparation for the audit should include identifying and verifying that appropriate documentation for the specific audit is available and accessible to the audit team. The feasibility of the audit should address issues such as availability and cooperation of key participants, adequate time and resources and sufficient records.

The Audit Plan

The audit plan is key to the success of the security audit. At a minimum, the Plan should include:

- *Audit objectives;*
- *Scope*
- *Methodology*
- *Criteria and references;*
- *List of audit roles and responsibilities; and an*
- *Audit schedule.*

The plan may also need to state issues related to confidentiality of information as well as handling and other protective measures as provided by applicable security guidance documents.

Conducting the Audit

During the conduct of the audit, the following steps should be included to the extent possible based on the approach and type of audit:

- *Initial meeting with participants and stakeholders;*
- *Collect and review documents, records and samplings;*
- *Provide status reports;*
- *Assess findings against established criteria; and*
- *Determine the audit conclusions.*

Example:

If the audit included assessing conformance to participating in security awareness sessions, the criteria at the outset would indicate the number of employees available, the number scheduled for participation and the content to be delivered. The audit team determines how many participated attended during the specified period based on records or samplings of other attendance information collected during the training and generates a finding of conformance or non-conformance based on percentages established at the beginning of the audit.

Producing the Audit Report

The audit team leader should generally prepare the audit report using impute from other team members. The audit report should provide a complete, accurate, concise and clear record of the audit, and should adhere to any pre-established audit report format. The format should include:

- *Objectives;*
- *Scope;*
- *Identify system or process(s) being audited;*
- *Document the criteria established for the audit;*
- *List of participants;*
- *Dates and Location(s) of the audit;*
- *Audit findings;*
- *Conclusions; and*
- *Statement on fulfillment of audit criteria.*

Depending on the initial mandate for the audit, recommendations may be appropriate. In addition, the report may indicate areas excluded from the audit as well as any implications for further audits.

Completing the Audit

The audit may be declared completed when all of the stated audit plan activities have been executed. If the audit is conducted by an external team, it may be required to return all documents and records that were collected for analysis and review.

Brief lessons learned report may be generated by the team if it is determined appropriate and facilitates a management review review and continual improvements.

Audit Follow-up

If follow-ups were deemed necessary or expected, they should be addressed in the report conclusions. At a minimum, an action report should be generated to track the status of improvements and any outstanding items from the report conclusions and/or recommendations.

Summary

Audits are necessary management process and they produce results that can be used to demonstrate conformance to security expectations and requirements. They provide management with an unbiased look at how well security controls and related processes are functioning. The results can be used to facilitate improvements or establish any necessary corrective actions.

Bibliography

BSI standards Publication, Guidelines for auditing management systems, ISO 19011:2011

ISACA, COBIT 5 A Business Framework for the Governance and Management of Enterprise IT

ISACA, COBIT 5 for Information Security, 2012

ISO Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO/IEC 27000:2016(E)

ISO Information technology — Security techniques —Information Security Management Systems – Requirements, ISO/IEC 27001:2013

ISO Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services, ISO/IEC 27017:2015

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014.