REFERENCE SHEET

CONDUCTING A SECURITY AUDIT

Purpose of this document

Even if you are very knowledgeable about security concerns and stay up to date on what's new in the field, nothing tops an external expert's viewpoint or opinion.

This document will help you determine which type of security audit to choose and how to prepare for it.

Why conduct a security audit?

Benefits for the organization

Conducting a security audits offers a number of tangible benefits. Here are some examples:

- Identify the strengths and weaknesses of the security measures currently in place
- Benefit from the knowledge of specialized security resources that provide advice and opinions specific to your organization and activity sector
- Raise awareness among senior management about the existence of control measures, how to apply them, and their effectiveness
- Reassure clients about your organization's governance in relation to security
- Set yourself apart from your competitors and respond to calls for tenders that have security audits as a requirement

Using an external independent auditor

Completing a self-assessment of security measures is possible, but relying on an independent external auditor means that the work completed is more credible. The choice of auditor depends on the type of report.

Different types of audit

A security audit report can meet one or more needs. These needs can be:

Regulatory

Depending on your activity sector, regulatory authorities may request or require a security audit report

Financial

When preparing financial statements, auditors require audit reports for the organization's external service providers

Reputational

Shows that you are properly managing your technology risks and controls

Credibility

An audit report containing an external opinion is a source of credibility that reassures management of your organization

Commercial

Since knowledge about safety has become a criterion for choosing suppliers of products and services, this will allow you to respond to a call for tenders as a goods and services provider.

Types of reports

There are several types of audit reports involving various standards. There is the SOC (System and Organization Controls) series of reports, ISO/IEC 27001, as well as specialized audits.

Here's a table summarizing the names, the organizations authorized to issue the reports, the scope, objectives, and audience of each type of report.

Table 1: Different audit reports

Name of audit report	Purpose of the audit report	Organization authorized to issue the report
SOC 1[1]	Demonstrate the suitability of the relevant controls to respond to financial audits or financial disclosure requirements (e.g. SOX, Regulation 52-109). Used to obtain an opinion from an independent external auditor on the creation and application of controls (type 1) and the effectiveness of the controls (type 2).	Accounting firms
SOC 2	Demonstrate the suitability of relevant controls for security, availability, processing integrity, confidentiality, and personal information protection. Used to obtain an opinion from an independent external auditor on the creation and application of controls (type 1) and the effectiveness of the controls (type 2).	Accounting firms
SOC 3	Based on *Trust Services Principles* and used primarily to demonstrate the existence of controls and for marketing purposes.	Accounting firms
ISO/IEC 27001	Used to obtain an assessment of the implementation of the information security management system in accordance with ISO 27002 standard criteria.	Firms or individuals with the necessary expertise and accreditation can issue this type of report
Specialized audits (e.g. PCI-DSS)	Used to obtain an assessment and results of the analysis of certain security-related elements such as vulnerability tests, discoveries of flaws, and compliance with the PCI-DSS standard.	Professional firms or individuals with cutting edge technical expertise in security can issue this type of report

[1] SOC 1 is also known as SSAE-18 or CSAE 3416

Major steps of an audit

Before the audit

Managers

- Plan the necessary resources (employees, budget, etc.)
- Authorize the audit (contractual commitment of the auditor)
- Determine the extent of the services to be audited
- Inform the Board of Directors

Employees

- Help determine the extent of the services to be audited
- Plan activities to assist the auditor
- Prepare the necessary documents

During the audit

Managers

- Follow up periodically on the progress of the audit and the potential shortcomings identified

Employees

- Assist the auditor to make their job easier

After the audit

Managers

- Read the report and sign it
- Conduct the post-mortem and document opportunities for improvement

Employees

- Distribute the reports to requesters
- Develop and monitor action plans, if necessary

How to prepare

Being well prepared helps reduce costs, make the auditor's job easier, and minimize gaps. Here are some activities to prepare for a security audit.

- Establish the organization's needs; this will determine the type of audit and report to be issued
- Beforehand, carry out a self-assessment of control measures to be audited
- Plan the time of year and availability of resources
- Establish the scope (extent) of services to be audited
- Prepare a budget (cost of the audit including the work of the individuals involved)

- Make sure at least one internal person has the required expertise
- Avoid hiring a person or firm that doesn't have the required expertise ((even your current accounting auditor may not have the required experience)

Learn more

Useful references:

- AICPA website on the topic of SOC
  https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html

- International Organization for Standardization (ISO) on the topic of the ISO/IEC 27001 standard: https://www.iso.org/isoiec-27001-information-security.html

- Accounting firms specialized in security that can issue SOC reports (non-exhaustive list):
  - PwC: https://www.pwc.com/ca/en.html
  - Deloitte: https://www2.deloitte.com/ca/en.html
  - E&Y: http://www.ey.com/home
  - KPMG: https://home.kpmg.com/ca/en/home.html
  - BDO: www.bdo.ca

- Other professional firms specializing in security (non-exhaustive list):
  - Infidem: https://infidem.biz/en/
  - GoSecure: http://gosecure.net
  - MNP: http://www.mnp.ca/