CHECKLIST

PERFORMING A SECURITY AUDIT

Purpose of this document

Even if you have a good understanding of security concerns and stay up to date in this area, the opinion of an external expert is irreplaceable in seeing where you stand.

This document will help determine what type of security audit to choose and how you should prepare.

Intended recipient: Manager and person responsible for the security of information systems.

Date of last modification: 2018-05

Why do a security audit?

Benefits for the organization

There are numerous tangible benefits to doing a security audit. Here are some examples:

- Identify the strengths and weaknesses of the security measures currently in place
- Take advantage of 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 efficiency
- Reassure your clients about your organization's governance in relation to security
- Stand out from the competition and respond to calls for tenders that have security audits as a requirement

Using an independent external auditor

Completing a self-evaluation 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**
  Based on the activity sector in which you work, the regulatory authorities can request or require a security audit report
- **Financial**
  When preparing financial statements, auditors require audit reports for the organization's external service providers
- **Reputational**
  To show that you are managing your risks and IT controls appropriately
- **Credibility**
  An audit report containing an external opinion is a source of credibility helping reassure the management of your organization
- **Commercial**
  As knowledge of security has become a criterion for selecting product suppliers and service providers, this will allow you to respond to calls for tenders as a supplier of products or provider of services

Types of reports

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

Below is a table that summarizes the names, organizations authorized to produce the report, scope, objectives and audience of each type of report.

Table 1: Different audit reports

Name of audit report	Objective and purpose of the audit report	Organization authorized to produce the report
SOC 1[1]	Show the suitability of the relevant controls to respond to financial audits or to the financial disclosure requirements (e.g. SOX, Multilateral Instrument 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	Show the suitability of the relevant controls for security, availability, processing integrity, confidentiality and the protection of personal information. 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 the Trust Services Principles; mostly used to show the existence of controls and for marketing purposes.	Accounting firms
ISO/IEC 27001	Used to obtain an evaluation of the implementation of an information security management system that conforms to the ISO 27002 standard.	Firms or individuals with the necessary expertise and accreditation can produce this type of report
Specialized audits (e.g. PCI-DSS)	Used to obtain an evaluation and the result of analyses for certain elements linked to security, such as vulnerability tests, the discovery of flaws and compliance with the PCI-DSS standard.	Professional firms or individuals with cutting-edge technical expertise in security can produce this type of report

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

Major steps of an audit

Before the audit

For managers

- Plan the necessary resources (staff, budget, etc.)
- Authorize the audit (contract undertaking of the auditor)
- Determine the extent of the services to be audited
- Brief the Board of Directors

For employees

- Collaborate to determine the extent of the services to be audited
- Plan activities to support the auditor
- Prepare the necessary documentation

During the audit

For managers

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

For employees

- Support and facilitate the auditor's work

After the audit

For managers

- Read and sign the report
- Complete the post-mortem and document areas for improvement

For employees

- Distribute the reports to the requesters
- Create and follow plans of action, if necessary

How to prepare

Being well prepared reduces costs, makes the auditor's work easier and minimizes gaps. Here's what to do to prepare yourselves for a security audit.

- Establish the organization's needs: this determines the type of audit and report to create
- Beforehand, complete a self-evaluation of the control measures to be audited
- Plan the time of year and availability of resources
- Establish the scope (extent) of the services to be audited

- Make a budget (cost of the audit including the work of the individuals involved)
- Insure that at least one internal staff member has the necessary expertise
- Avoid hiring a person or firm that does not have the necessary expertise (even your current accounting auditor may not have the required experience)

For more information

Some practical references:

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

- International Organization for Standardization (ISO) website 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 produce 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 specialized in security (non-exhaustive list):
  - Infidem: https://infidem.biz/en/
  - GoSecure: http://gosecure.net/
  - MNP: http://www.mnp.ca/