**Audit checklist**

It’s necessary to create an audit checklist before conducting an audit. A checklist is generally made up of the following areas of focus:

**Identify the scope of the audit**

* The audit should:
  + List assets that will be assessed (e.g., firewalls are configured correctly, PII is secure, physical assets are locked, etc.)
  + Note how the audit will help the organization achieve its desired goals
  + Indicate how often an audit should be performed
  + Include an evaluation of organizational policies, protocols, and procedures to make sure they are working as intended and being implemented by employees

**Complete a risk assessment**

* A risk assessment is used to evaluate identified organizational risks related to budget, controls, internal processes, and external standards (i.e., regulations).

**Conduct the audit**

* When conducting an internal audit, you will assess the security of the identified assets listed in the audit scope.

**Create a mitigation plan**

* A mitigation plan is a strategy established to lower the level of risk and potential costs, penalties, or other issues that can negatively affect the organization’s security posture.

**Communicate results to stakeholders**

* The end result of this process is providing a detailed report of findings, suggested improvements needed to lower the organization's level of risk, and compliance regulations and standards the organization needs to adhere to.