Audits and Assessments

Security Architecture & Tool Sets

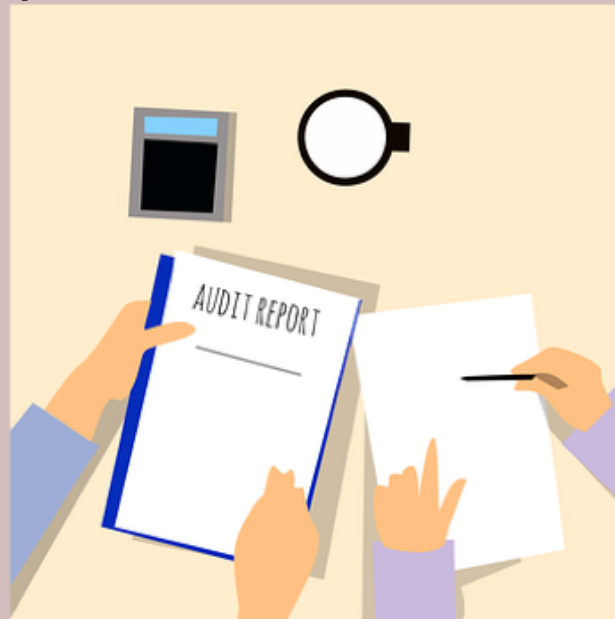# Quality Control

- Louis V. Gerstner, former IBM Chairman

  You get what you inspect,
  not what you expect…

- Evaluation of your cybersecurity program is essential to it being effectively run

- Evaluation occurs as audits or assessments

Audits

- Formal review of organizational cybersecurity program (internally)

- Or, it can be for a specific compliance requirement (externally), like PCI DSS

- Rigorous, formal testing of controls resulting in formal declaration by the auditor of compliance

Assessments

- Less formal review of security controls

- Usually request by the organization itself for process improvement purposes

- Information gathered through interviews with employees (which is considered the truth) instead of independent verification