The purpose for the below is for IT HIPAA audit compliance and report generation and remedying, also known as an SRA – Security Risk Analysis.

The information should be sent to a server or to the local laptop. Generate a full report of compliance vs non-compliance. Options for a “Resolve” and “Undo” button one at a time or option to do all at once. The below is the current list I have of items I am looking for.

Since this is a discovery process. I need to verify this is the appropriate way to do this project and if there are objects I am missing that should be inside the report. The report ideally should have a before and after compliance check list, with graphs, pie charts to give the client a visual representation of their network. The report will be ran once a year for the client

User accounts

* Check user and security groups. Must verify users have appropriate access

GPO

* Generate GPOs and policies report on workstations and servers
* Enforce strong passwords
* Auto logout after 15 minutes at idle
* Password prompts on screen saver
* Audit enabled on workstation and server
* GPO macros deny for Microsoft Office
* Enforce Strong passwords
* .js with notepad and blocking executables from running in the default zip deflate locations

Powershell

* Generate local and server user and security group list
* Pull server and workstation records for Disk space, RAM, PC name, and serial number on network through WMI/SNMP.
* Check if SMB1 is enabled
* Network folder share, permissions, and user/groups

Network – later use

* Check Vlan groups
* Port opens on firewall
* Check enabled ports
* Check heavy flow of traffic

Documentation

* https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise
* 11) Planning for compromise - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/planning-for-compromise
* 12) Audit policies --- https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
* 13) https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory