Common Issues seen before the on-site review

- Changing settings on local machines (e.g. disable lockdown mode, enable SSH, open ports, etc.).
- Registry keys and other configuration elements need to be explicitly set and configured to meet Safeguards requirements. Using defaults or unconfigured items can lead to Nessus determining a NULL result which cannot be accepted.
- Ensuring credentials with the appropriate level of permissions are created and entered per the Nessus prep package guidance.
- Define network location for scanning, whitelist scan engine.
- Taking down or whitelisting firewalls.
- Ensure test scans prior to the on-site visit are successful by validating the existence of “Compliance Details” for each host. Compliance details must be gathered for Safeguards to complete the assessment.
- Please do not combine technologies in the same family (e.g. - Windows 7, 8.1, 10). One scan (or more if needed) per operating system is needed to complete reporting requirements.

Common issues seen during the on-site review

- Turn off host protection software.
- Ensure availability of staff during scans.
- Common Issues for Nessus scans:
- Windows
  - Local accounts were used but the LocalAccountTokenFilterPolicy registry key was not set to ensure Local Administrator accounts can access the remote registry.
- Linux/Unix
  - Proper root equivalency through elevation is not achieved.
- Database
  - Oracle – Improper SID is entered.
  - SQL Server – Instance name is incorrect. Removing instance name from scan may be required.
  - All – Appropriate active node IP address or Virtual IP (VIP) is not provided.
- VMware
  - Errors in the form of NULL results are returned if Nessus is virtualized in the same instance that is being scanned.