Checklist to achieve PCI Compliance

☐ *Annually verify the PCI scope*

Annually update a document which lists the scope of PCI for the appropriate areas.
- Places
- People
- Business processes for receiving and processing Credit Card payments
- All systems used to process Credit Card transactions
    - Phone systems
    - Computers, workstations, networks, etc.
    - Credit Card Terminals

☐ *Annual PCI Risk Assessment*

Annually, using the PCI scoping documents, create a Risk Assessment for the organization using the NIST process or another approved process.

☐ *Train users*

Verify that users have been trained on how to protect PCI.

☐ *Monthly vulnerability scans*

If any computers or VOIP systems are used to process credit cards, then make sure that the systems are scanned at least monthly and that changes are made to systems to fix the vulnerabilities which are found.

☐ *Continue to make changes to processes and systems*

Using the PCI scoping documents, start making changes to systems and processes to comply with the various PCI-DSS requirements.

☐ *Annually update the SAQ*

The Self-Assessment Questionnaire should be updated at least annually and submitted to the monitoring organizations.