# PCI DSS v4.0.1 Audit Plan

**1. Planning and Scope Definition**

- **1.1. Engagement Letter and Scope Definition:**
  - Obtain a signed engagement letter that clearly defines the scope of the assessment, including:
    - The Cardholder Data Environment (CDE).
    - All system components, people, and processes involved in cardholder data.
    - The time period covered by the assessment.
    - The specific PCI DSS version (4.0.1).
    - Roles and responsibilities of the auditor and the entity being audited.
  - Document the scope in detail, including network diagrams, data flow diagrams, and lists of systems and applications.
  - Identify all third-party service providers involved in the CDE and their PCI DSS compliance status.
- **1.2. Risk Assessment:**
  - Conduct a preliminary risk assessment to identify potential areas of non-compliance.
  - Review previous audit reports and remediation plans.
  - Analyze the entity's risk management policies and procedures.
  - Determine the level of effort and resources required for the audit.
- **1.3. Audit Team Formation:**
  - Assemble a qualified audit team with the necessary PCI DSS expertise.
  - Ensure the team is independent and free from conflicts of interest.
  - Assign specific responsibilities to each team member.
- **1.4. Audit Plan Development:**
  - Develop a detailed audit plan, including:
    - The audit objectives.
    - The audit methodology.
    - The audit schedule.
    - The sampling strategy.
    - The documentation requirements.
    - The communication plan.
- **1.5. Document and Information Request:**
  - Create a request list for all documentation required. This includes, but is not limited to:
    - Policies and procedures.
    - Network diagrams.
    - System configuration documentation.
    - Change management records.
    - Incident response plans.
    - Access control lists.
    - Vulnerability scan reports.
    - Penetration testing results.

**2. Data Gathering and Review**

- **2.1. On-Site Visits and Interviews:**
  - Conduct on-site visits to observe the CDE and interview key personnel.
  - Interview system administrators, network engineers, application developers, and security personnel.
  - Document all interview findings.
- **2.2. Document Review:**
  - Review all documentation provided by the entity.
  - Verify that policies and procedures are up-to-date and accurately reflect the entity's practices.
  - Assess the effectiveness of the entity's security controls.
- **2.3. System Configuration Review:**
  - Review the configuration of all system components in the CDE.
  - Verify that systems are configured according to PCI DSS requirements.
  - Check for default passwords, unnecessary services, and other security vulnerabilities.
- **2.4. Network Security Assessment:**
  - Review the network security architecture, including firewalls, routers, and intrusion detection/prevention systems.
  - Verify that network segmentation is implemented effectively.
  - Review wireless network security controls.
- **2.5. Vulnerability Scanning and Penetration Testing:**
  - Review the results of vulnerability scans and penetration tests.
  - Verify that vulnerabilities are remediated in a timely manner.
  - Assess the effectiveness of the entity's vulnerability management program.
- **2.6. Cardholder Data Discovery:**
  - Utilize tools to locate all locations where cardholder data is stored, processed, or transmitted.
  - Verify that all identified locations are included in the scope of the audit.
  - Verify that any unnecessary storage of cardholder data is removed.
- **2.7. Review of Cryptography:**
  - Verify that strong cryptography is used to protect cardholder data in transit and at rest.
  - Verify that key management procedures are in place.
  - Verify that cryptographic algorithms and key lengths are compliant with PCI DSS requirements.
- **2.8. Review of Change Management:**
  - Review the entity's change management procedures.
  - Verify that changes to the CDE are properly authorized and documented.
  - Verify that changes are tested and implemented in a controlled manner.
- **2.9. Review of Incident Response:**
  - Review the entity's incident response plan.
  - Verify that the plan is up-to-date and addresses all relevant threats.
  - Verify that incident response procedures are tested regularly.
- **2.10. Review of Logical and Physical access controls:**
  - Verify that access to the CDE is restricted to authorized personnel.
  - Verify that access control procedures are in place and effective.
  - Review physical security controls, such as access badges, surveillance cameras, and alarm systems.

- **2.11. Review of Security Awareness Training:**
  - Verify that all personnel involved in the CDE receive regular security awareness training.
  - Verify that training covers PCI DSS requirements and the entity's security policies.
- **2.12. Review of Third-Party Service Providers:**
  - Verify that third-party service providers are PCI DSS compliant.
  - Review contracts and service level agreements.
  - Review the third party providers Attestation of Compliance(AOC).
- **2.13. Review of Logging and Monitoring:**
  - Verify that system logs are collected and monitored.
  - Verify that security events are investigated and resolved.
  - Verify that intrusion detection/prevention systems are configured correctly.
- **2.14. Review of Timely remediation of vulnerabilities:**
  - Verify that the entity is addressing vulnerabilities in a timely manner.
  - Verify that a process is in place to track and remediate vulnerabilities.

**3. Testing and Validation**

- **3.1. Sample Testing:**
  - Conduct sample testing of security controls to verify their effectiveness.
  - Test access controls, network security controls, and application security controls.
- **3.2. Evidence Collection:**
  - Collect evidence to support audit findings.
  - Document all test results and observations.
  - Obtain screenshots, log files, and configuration files as needed.
- **3.3. Validation of Compensating Controls:**
  - If compensating controls are used, verify that they meet PCI DSS requirements.
  - Ensure that they are documented and properly implemented.

**4. Reporting and Remediation**

- **4.1. Audit Findings Documentation:**
  - Document all audit findings in a clear and concise manner.
  - Identify the specific PCI DSS requirements that are not met.
  - Provide recommendations for remediation.
- **4.2. Report of Compliance (ROC) or Self-Assessment Questionnaire (SAQ) Completion:**
  - Complete the ROC or SAQ, as applicable.
  - Ensure that the report is accurate and complete.
  - Provide all required supporting documentation.
- **4.3. Remediation Planning:**
  - Work with the entity to develop a remediation plan.
  - Establish timelines for remediation activities.
  - Monitor the progress of remediation.
- **4.4. Final Report Submission:**
  - Submit the final audit report to the entity and the acquiring bank or payment brand, as required.
  - Retain all audit documentation for the required retention period.
- **4.5. Follow-Up Reviews:**
  - Conduct follow-up reviews to verify that remediation activities have been completed.
  - Verify that the entity maintains ongoing PCI DSS compliance.

**Key Considerations for PCI DSS v4.0.1:**

- **Targeted Risk Analysis (TRA):** Ensure that the entity conducts thorough TRAs for all requirements.
- **Customized Approach:** Ensure that the audit is customized to the entity's specific environment.
- **Evolving Technologies:** Stay up-to-date on evolving technologies and their impact on PCI DSS compliance.
- **Accountability:** Verify that roles and responsibilities are clearly defined.
- **Accuracy:** Verify that all documentation is accurate and up-to-date.
- **Documentation:** Ensure that all documentation is maintained according to PCI DSS requirements.
- **Continuous Monitoring:** Verify that the entity has continuous monitoring in place.
- **Authentication:** Verify that strong multi-factor authentication is being used.
- **Password Complexity:** Verify that strong password complexity is being used.
- **Service Provider Management:** Verify that service providers are being managed appropriately.