

1. PCI DSS Compliance Workflow

- 

1. Scope Identification

Define the Cardholder Data Environment (CDE), data flows, and third-party connections.
- 

2. Readiness Assessment

Define the Cardholder Data Environment (CDE), data flows, and third-party connections.
- 

3. Remediation

Fix vulnerabilities, update configurations, implement missing controls.
- 

4. Validation

Undergo QSA-led RoC or complete SAQ; confirm evidence.
- 

5. Certification

Submit AoC/SAQ to acquiring bank or payment brand.
- 

6. Continuous Monitoring

Use GhostWatch to maintain compliance year-round.

Based on PCI DSS v4.0.1

2. PCI DSS Audit Preparation Checklist

Before Audit

- Confirm scope (Req 12.5)
- Update network and data flow diagrams (Req 1.1.3)
- Collect scans, pen-test results, logs, and change records (Req 11.x)
- Review and approve security policies (all requirements)
- Verify training completion (Req 12.6)

During Audit

- Provide evidence samples and screenshots
- Support QSA interviews and technical walkthroughs

After Audit

- ✔ Keep compliance status constantly
- ✔ Feed regular tasks results into GhostWatch for continuous monitoring

Retain audit evidence for ≥ 12 months (24 months recommended)



2. PCI DSS Audit Preparation Checklist

PCI DSS v4.0.1 – The 12 Pillars of Payment Card Security.

- 

1. Install and maintain network security controls
- 

2. Apply secure configurations to all system components
- 

3. Protect stored account data
- 

4. Protect cardholder data in transit over public networks
- 

5. Protect systems and networks from malware
- 

6. Develop and maintain secure systems and software
- 

7. Restrict access to system components and cardholder data by need-to-know
- 

8. Identify users and authenticate access to system components
- 

9. Restrict physical access to cardholder data
10. Log and monitor all access to system components and cardholder data
- 

11. Test security systems and processes regularly
- 

12. Support information security with organizational policies and programs