

12 Critical items across facility, process, compliance, lifecycle, and chain of custody.

- ☐ FACILITY Key injection performed at a PCI-certified facility
- ☐ HARDWARE Hardware security modules [HSMs] used for key generation and storage
- ☐ PROCESS Dual control and split knowledge protocols enforced
- ☐ TRANSPORT keys encrypted during transport [clear-text only under strict PCI dual control]
- ☐ CONFIG. Unique key assignment per device verified
- ☐ VERIFICATION Post-injection transaction testing completed
- ☐ COMPLIANCE Full audit trail with device serial numbers and timestamps
- ☐ LIFECYCLE Key rotation schedule defined and documented
- ☐ LIFECYCLE PCI PTS Device expiration dates tracked
- ☐ HARDENING Terminal hardening completed [Firmware lock, port restrictions]
- ☐ PHYSICAL Physical tamper protections verified
- ☐ CHAIN Chain of custody documented from procurement to deployment

10-12 CHECKED

Your security posture is strong. Resolve any remaining items and ensure documentation is audit-ready.

10-17 CHECKED

Each unchecked item is a potential audit finding or security vulnerability. Prioritize before your next deployment wave.

0-9 CHECKED

Processes need major strengthening. Engage a PCI-certified partner before devices enter a live payment environment.