



Security
Standards Council®

PCICOMPLYHUB GRC PLATFORM - PCI DSS V4.1 COMPLIANCE

Presented to:

Dr: Muhammad Hataba

Proposal by :

Yasser Mohamed : 320220211

Mark Adly : 320220212

Gehad Abdellah : 320220237

OVERVIEW

PCIComplyHub streamlines PCI DSS v4.1 compliance by importing official controls, mapping them to assets like ATMs and servers, calculating maturity scores, and generating PCI-specific audit reports.

Tailored for Linux/Kali users, it uses SSH for secure evidence collection from PCI-scoped systems without multi-framework distractions.



CORE FEATURES

- **Framework Import:** Loads PCI DSS v4.1 controls directly from official PCI SSC JSON schemas or documents for accurate, up-to-date requirement coverage.
- **Control Mapping:** Automates tagging of the 12 PCI DSS requirements against network assets, CDE boundaries, and configurations using JSON rules and scans.
- **Compliance Scoring:** Assigns 0-5 maturity levels per control with real-time dashboards, heatmaps, and remediation prioritization for PCI gaps.
- **Exportable Summaries:** Produces SAQ, ROC, and POA&M reports in PDF/CSV with embedded evidence links tailored for PCI auditors.



TECHNICAL IMPLEMENTATION

- Python core for scoring and data aggregation; Bash for Linux scripting and SSH integrations.
- PySimpleGUI for cross-platform dashboards with CLI fallback for advanced Kali/NixOS users.
- Docker deployment for easy setup in test or production networks.

Requirement	Implementation
Framework Import	PCI DSS v4.1 JSON from official sources pcisecuritystandards
Control Mapping	Asset scanning and PCI-specific tagging cynomi
Compliance Score	Maturity dashboard with PCI heatmaps compliancemanagergrc
Export Summary	PCI SAQ/ROC/POA&M with evidence drata

CONCLUSION

In cybersecurity environments handling payment systems like ATMs, maintaining PCI DSS v4.1 compliance demands efficient tools that cut through complexity. PCIComplyHub emerges as a lightweight GRC platform dedicated exclusively to this standard, importing its 12 core requirements directly from official PCI SSC JSON schemas for precise alignment. Tailored for Linux experts using Kali or NixOS, the tool automates control mapping across network assets and CDE boundaries via SSH-secured scans, eliminating manual drudgery while ensuring evidence collection from scoped servers remains secure and auditable.

The platform's strength lies in its real-time compliance engine, which scores each control on a 0-5 maturity scale and visualizes gaps through intuitive heatmaps and dashboards powered by PySimpleGUI. Users gain actionable insights—prioritizing remediation for high-risk areas like segmentation failures—before exporting audit-ready SAQ, ROC, or POA&M reports in PDF/CSV formats complete with evidence links. Deployed via Docker, it fits seamlessly into VM testing workflows, starting with a CLI MVP achievable in two weeks and evolving to full GUI by Q1 2026.