Cybersecurity & Compliance Assessment

PCI DSS Concepts • Risk Assessment • Security Governance

PCI DSS Concepts	Risk Assessment	Firewall Review	MFA

Overview

This case study shows the ability to assess business security gaps, organize findings, and recommend remediation steps in a format business leaders can understand.

Business Challenge

Businesses that handle sensitive data need documented security controls, access policies, firewall rules, monitoring, and compliance awareness. Gaps can lead to downtime, data exposure, fines, and loss of customer trust.

Example Solution

A security assessment approach was used to review access control, firewall configuration, authentication practices, monitoring, and data protection requirements. Findings were converted into practical remediation themes.

Technologies / Methods Demonstrated

- PCI DSS Concepts
- Risk Assessment
- Firewall Review
- MFA
- Policy Development
- Access Control
- Security Documentation

Business Outcomes

- Identified compliance and operational risk areas.
- Converted technical findings into business-impact language.
- Created a remediation path focused on access, segmentation, documentation, and monitoring.

What This Shows a Client

- Shows compliance awareness.
- Shows ability to communicate risk clearly.
- Shows business-focused cybersecurity thinking.

Details intentionally not published

- Full audit worksheets.
- Client-sensitive findings.

- Exact infrastructure weaknesses.
- Internal questionnaires and scoring details.

This document is designed to give website visitors confidence in EPIC TECH LLC capability without publishing full implementation playbooks or reusable client deliverables.