FIELD ASSESSMENT REPORT

GRC REPORT

NIST 800-53 | ISO/IEC 27001 | SOC 2 | PCI-DSS

2025

Franchise Owner: WIT LLC
Store Location: Florissant, MO
Assessed by: Abinav Joshi – GRC Analyst
Date of Visit: July 11, 2025
Report Created: July 11, 2025
Scope: GRC analysis of one Boost Mobile retail store under WIT LLC, which operates six branches in Missouri.

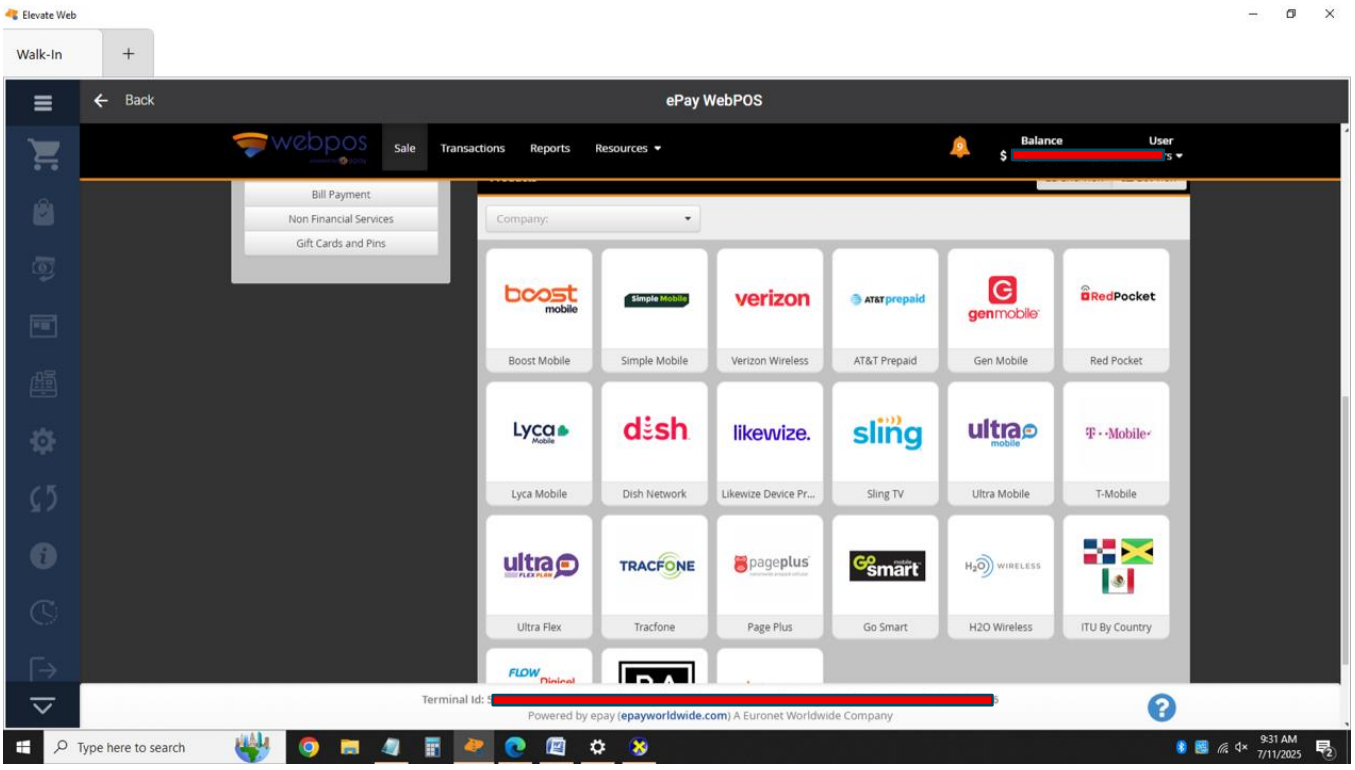
1. Introduction

As part of a Governance, Risk, and Compliance (GRC) learning and portfolio-building initiative, I visited a Boost Mobile franchise store located near the St. Louis Lambert International Airport. This store is one of six operated by WIT LLC. I sought permission from the store manager, Mr. Sarmad Raheel, to observe the systems and processes in use. Mr. Raheel granted me access to the front desk Windows PC used by sales agents, which also runs all core business systems.

The objective of this assessment was to observe the operational environment, identify GRC-related concerns, and map them to known frameworks such as NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and SOC 2 Trust Services Criteria.

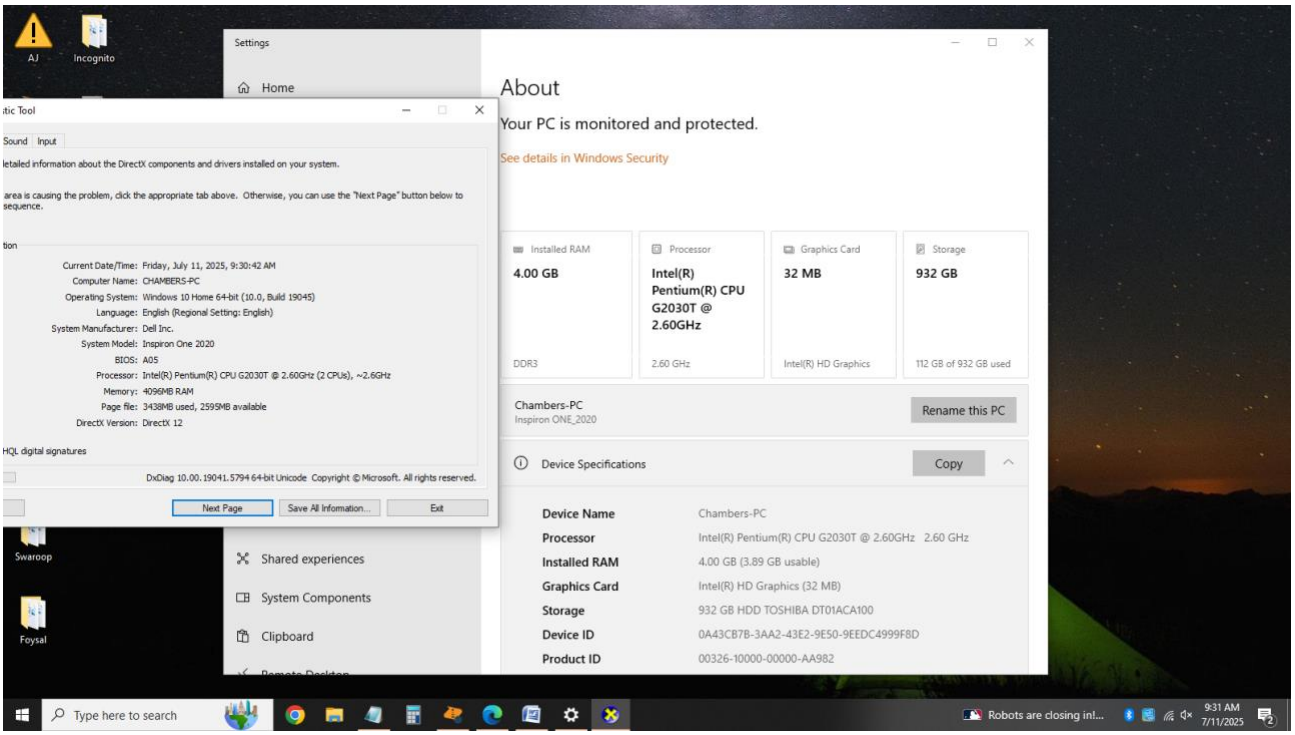
2. Systems & Applications Observed

- **Elevate:** Boost Mobile's internal platform used for business functions such as bill payments, device upgrades, adding lines, and customer info lookup.
- **ePay WebPOS:** A web-based platform integrated with Elevate to process payments for major U.S. carriers (e.g., AT&T, T-Mobile, Verizon)



- **Clover POS:** Used for in-store purchases. Records payment transactions and prints receipts.

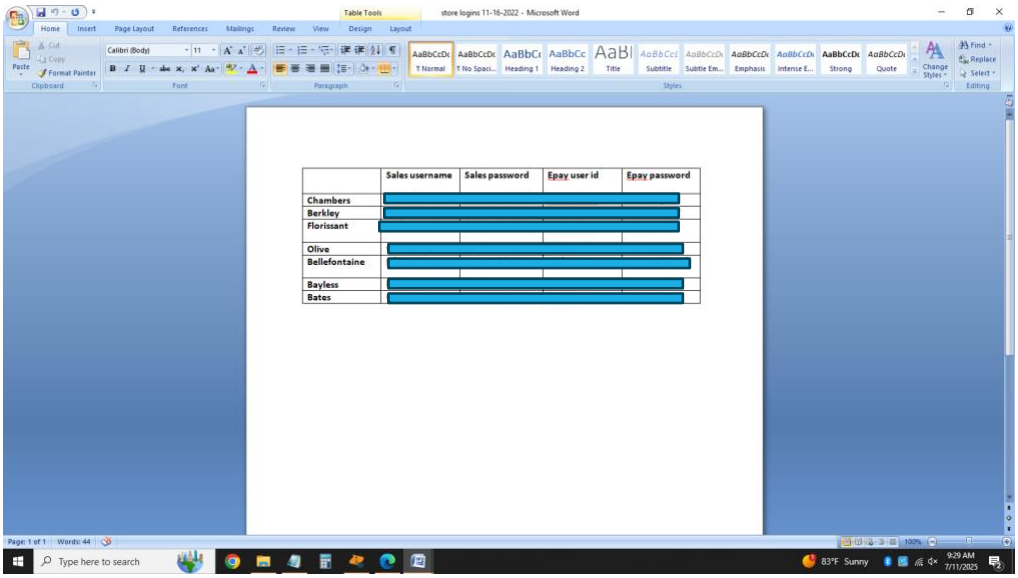
- **Windows Desktop System:** Runs Windows 10 Home on an outdated Intel Pentium G2030T CPU with 4GB RAM and no third-party antivirus.

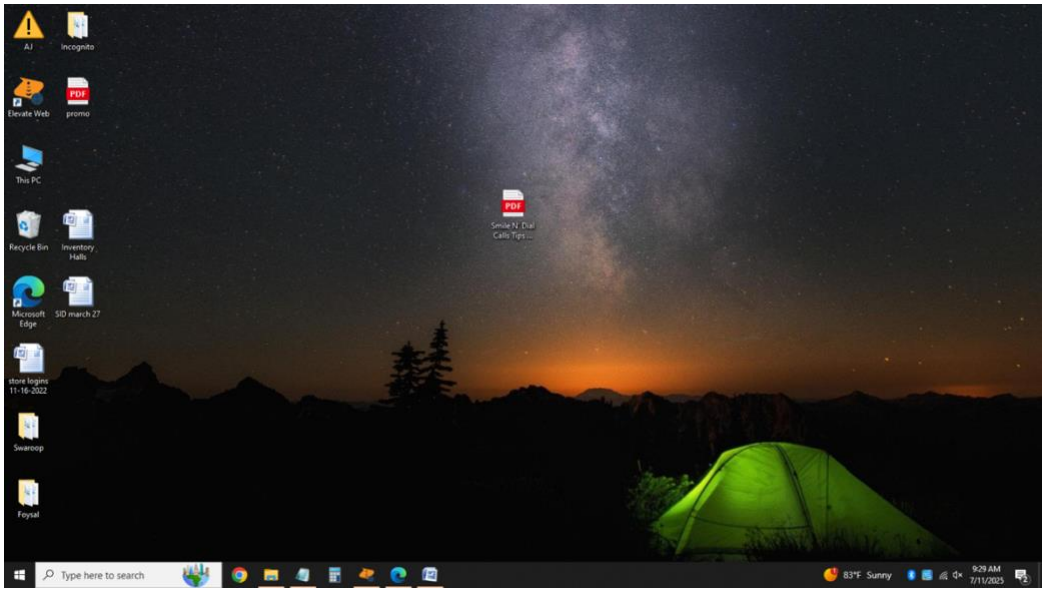


3. Observations from the Visit

3.1 Device Access & Physical Security

- The front-desk PC was active and unlocked.
- Sticky notes containing login credentials were posted directly on the monitor.
- A Word file named “store logins 11-16-2022” containing usernames and passwords for all six stores was saved on the desktop





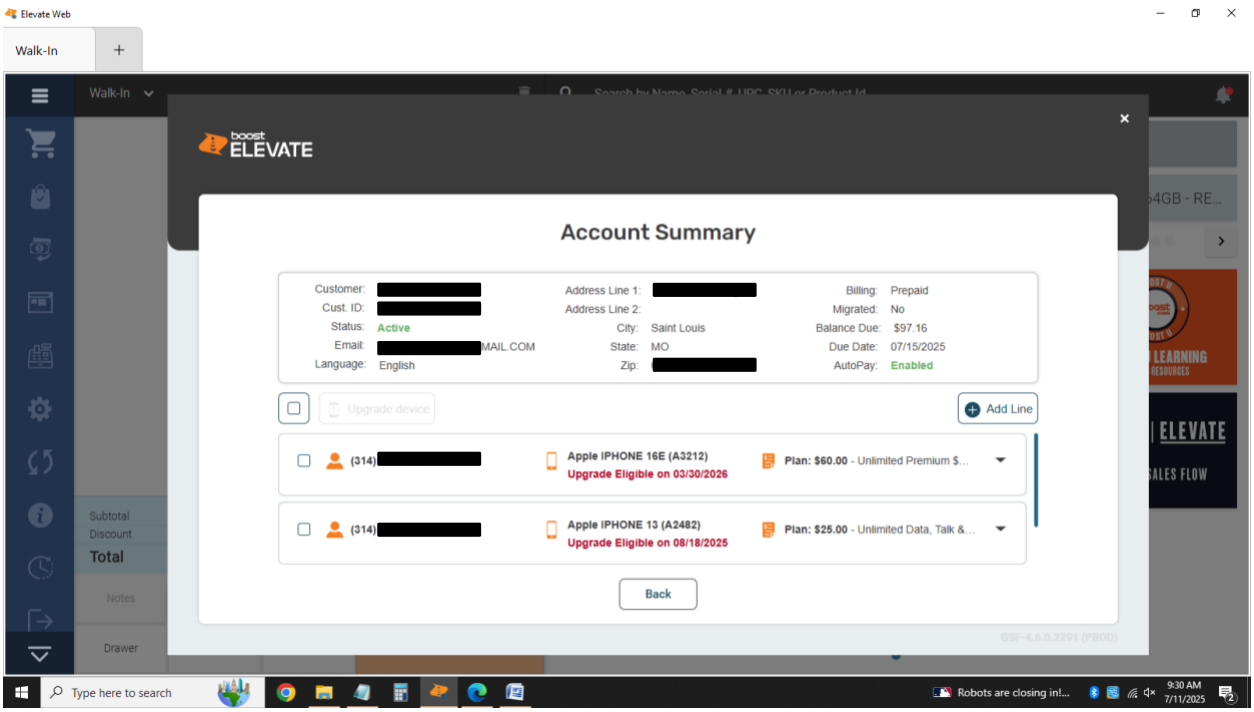
- The computer hardware was outdated and lag prone. No BIOS or boot password protection was observed.

3.2 Software & Network

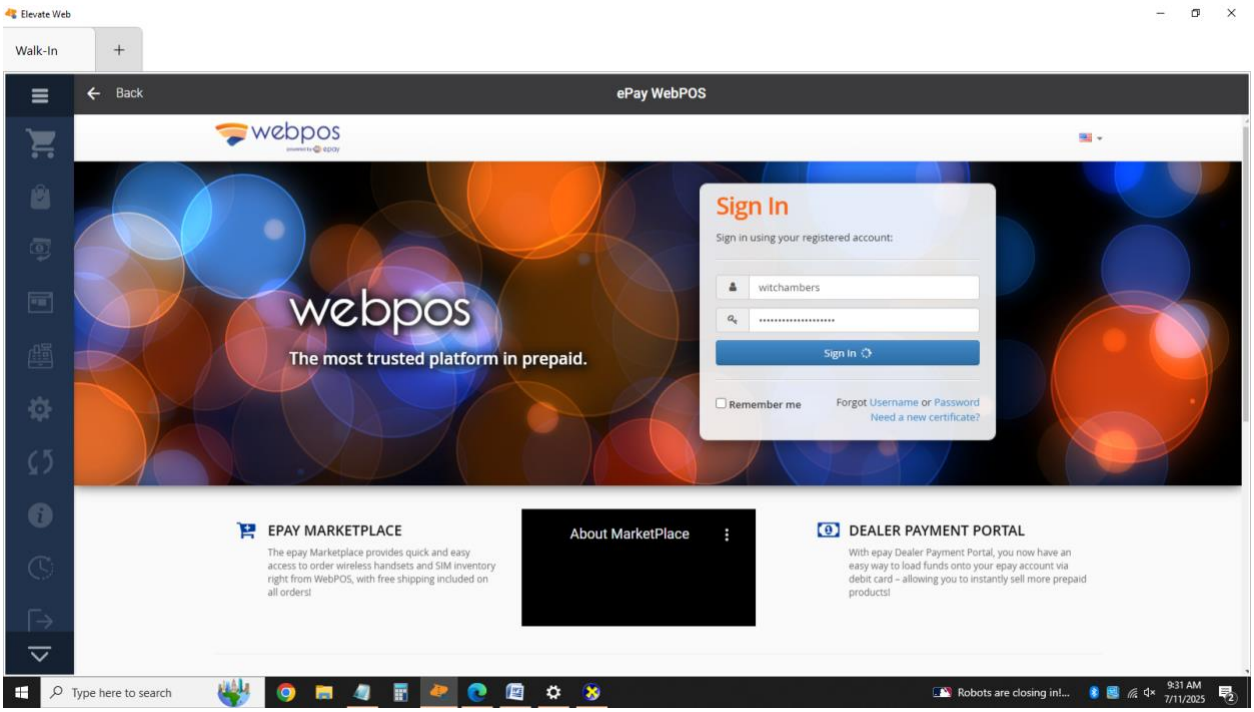
- Only Windows Defender was active; no third-party antivirus or EDR (Endpoint Detection and Response) installed.
- System appeared outdated with no visible patch management or update enforcement in place.

3.3 Application Usage

- In Elevate, customer records (including name, address, plan info, and billing status) could be accessed by simply entering their phone number.
- Devices sold to customers came with factory PINs (commonly “1010”) that were never changed.



- A shared ePay login (“witchambers”) was used across multiple stores, with the password stored autofilled.

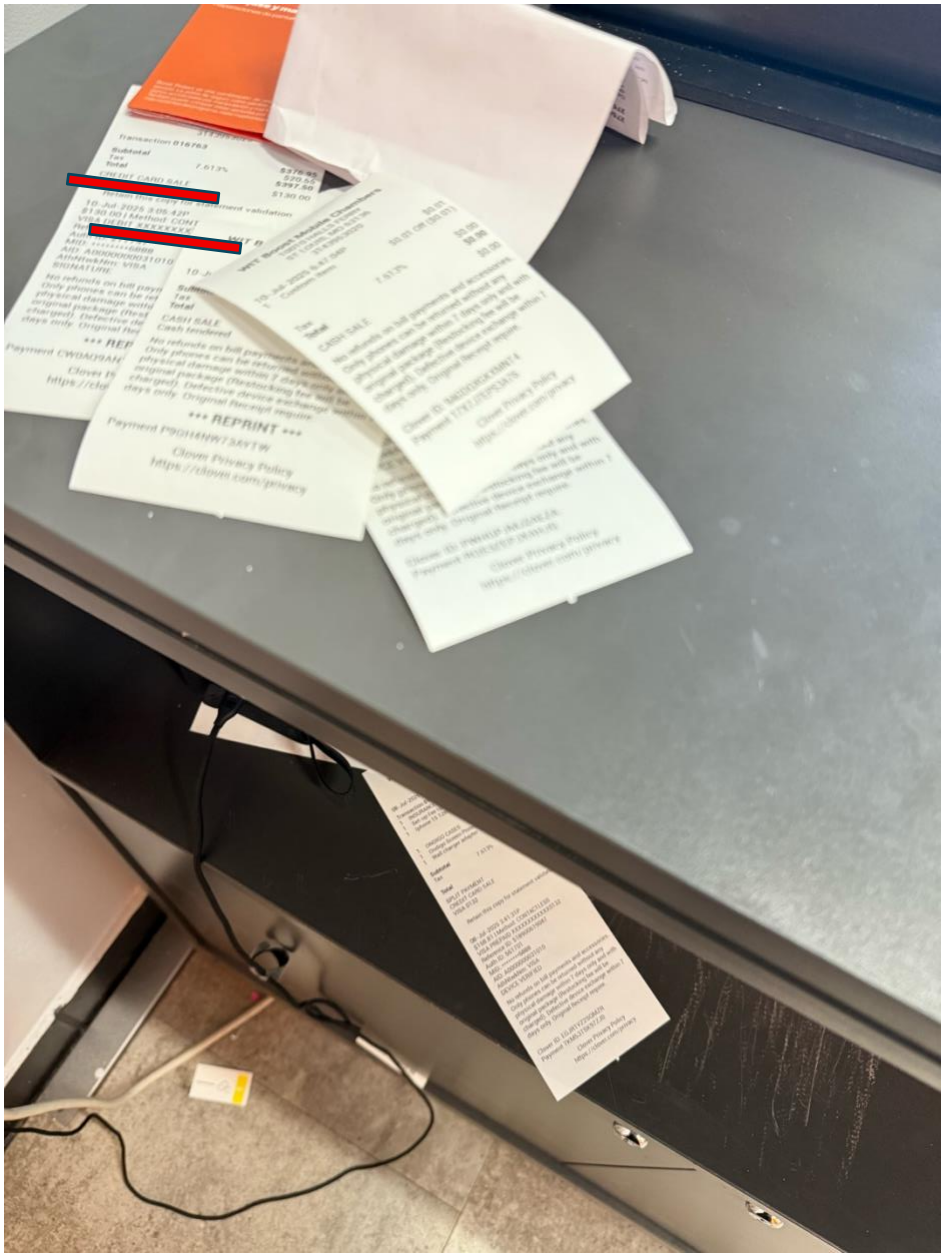


- Clover POS allowed *guest login* access without credentials.

3.4 Data Privacy Concern

- Due to the store’s proximity to the airport—and with the recent addition of nonstop flights from Germany to St. Louis—European tourists frequently purchase phones and SIM cards during their stay. As a result, personal data of EU citizens is often collected and stored in the Elevate system. Under the General Data Protection Regulation (GDPR), such data must be processed lawfully and not retained longer than necessary. Without a defined retention or deletion policy, the store risks noncompliance with GDPR’s core principles, including the right to erasure and storage limitation.
- Their information remains in Elevate indefinitely, with no formal data retention or deletion policy in place.

- Clover POS receipts did not show full card numbers (PCI-DSS compliant), but customer names were visible if previously saved



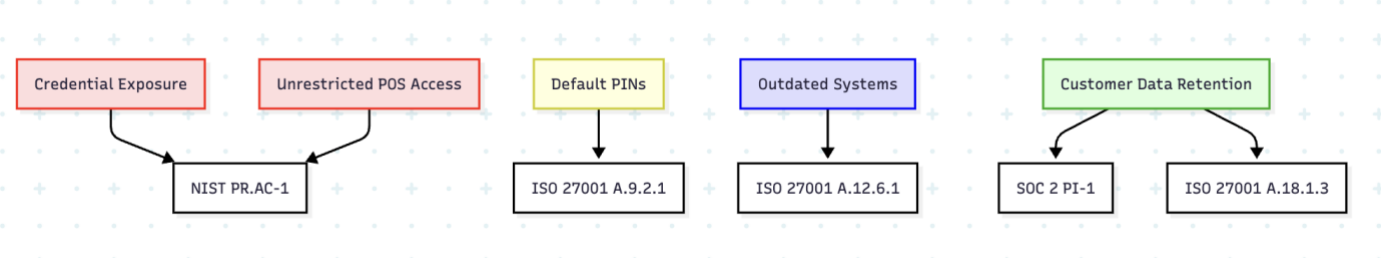
4. Governance, Risk & Compliance (GRC) Analysis

4.1 Governance

- **Policies & Documentation:** No written cybersecurity policy, data privacy policy, or access control policy observed.
- **Asset Management:** No formal inventory tracking system in place.
- **Roles & Responsibilities:** No use of role-based access controls. Shared credentials were common.
- **Change Management:** No documentation or process tracking for software or system updates.

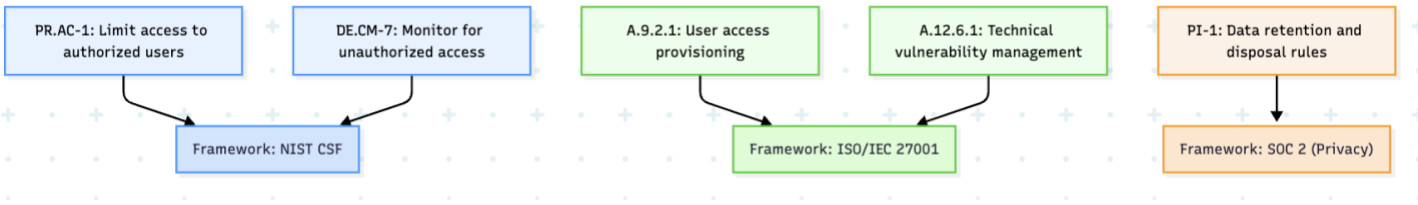
4.2 Risk Assessment

Risk	Description	Severity	Likelihood
Credential Exposure	Passwords stored in plain text and on sticky notes	High	High
Default PINs	Devices sold with unchanged factory PINs	Medium	High
Outdated Systems	Old PC hardware with no patching or modern security tools	Medium	Medium
Unrestricted POS Access	Guest access on Clover POS without authentication	High	High
Customer Data Retention	Personally identifiable information stored without retention rules	High	Medium



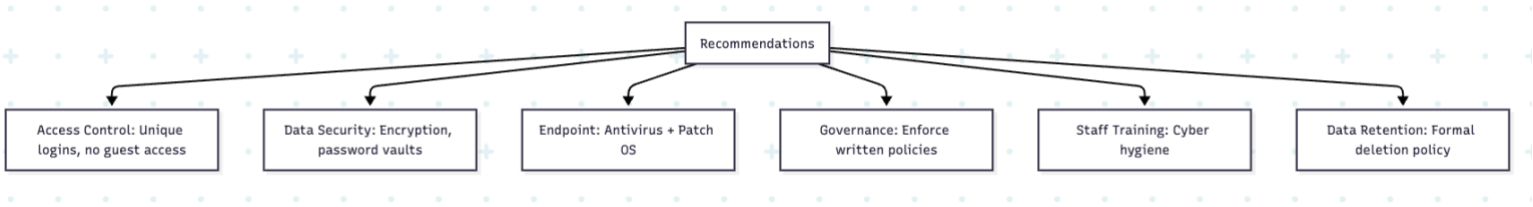
4.3 Risk Mapping to Frameworks

Control	Description	Framework Reference
PR.AC-1	Limit access to authorized users	NIST CSF
A.9.2.1	User access provisioning	ISO/IEC 27001
A.12.6.1	Technical vulnerability management	ISO/IEC 27001
DE.CM-7	Monitor for unauthorized access	NIST CSF
PI-1	Establish data retention and disposal rules	SOC 2 (Privacy)



5. Recommendations

Category	Action Item	Framework Reference
Access Control	Enforce unique logins and remove guest access	NIST PR.AC-1
Data Security	Encrypt sensitive files; implement password vaults	ISO 27001 A.10, NIST PR.DS
Endpoint Protection	Install antivirus and update OS patches regularly	NIST DE.CM-7, ISO A.12.6.1
Governance	Draft and enforce security, usage, and access policies	NIST ID.GV
Staff Awareness	Train employees on cybersecurity hygiene	NIST PR.AT
Data Retention	Define clear data retention/deletion policy	ISO A.18.1.3



6. Conclusion

Following my assessment, I advised the board managers at the Boost Mobile franchise (WIT LLC) on multiple critical compliance and security gaps observed during the visit. Recommendations included requiring customers to change default device PINs (e.g., from 1010 to a custom secure PIN) at the point of sale, implementing an inventory management system (preferably cloud-based) with unique login credentials for all users, and adopting a Zero Trust security policy to restrict access based on continual verification.

I also emphasized the need to install reputable antivirus software across all endpoints and begin a phased upgrade of outdated PC hardware to improve system performance and security resilience. These actions, combined with the adoption of structured frameworks like NIST CSF and ISO 27001, will not only enhance operational efficiency but also significantly strengthen the store's compliance posture and customer trust.

Establishing formal IT policies, training staff on security awareness, and conducting regular risk assessments are essential next steps in building a secure and compliant retail environment.