Audit scope:
● Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
● Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
● Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
● Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
● Ensure current technology is accounted for. Both hardware and system access.

Audit goals:
● To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
● Establish a better process for their systems to ensure they are compliant
● Fortify system controls
● Implement the concept of least permissions when it comes to user credential management
● Establish their policies and procedures, which includes their playbooks
● Ensure they are meeting compliance requirements

***critical findings*:**
- Least privilege and separation of duties : Giving vendors and employees the least average that they need to get their job done.
- Disaster recovery plans need to be implemented to ensure systems are able to run in the event of an incident
- Password policy: establish password strength rules to improve security and their management.
- Account management policies: Reduce attack surface to limit overall impact incase of an intrusion or abuse.

Findings:
- Betterment of access control policies: increase confidentiality,access and integrity of data.
- Implementation of systems: Intrusion detection system, Manual monitoring , maintenance and intervention, Firewalls need to be put in place to maintain security.

summary/recommendations:
- All rules, regulations and schemes should be in accordance with National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
- High priority tasks should be implemented followed by medium and low priority tasks.

- Data security should be the highest priority for the company, to avoid financial, reputational losses.