Capstone Project Solution: Recommendations.

The following are a set of recommendation based on the NIST assessment that you conducted.

The recommendations should be prioritised in order of importance.

Key Areas of Improvements:

➔ Cyber Security Governance:

- Hire a Cyber security manager or a Chief information security manager.
- Formalise cyber security roles and responsibilities. Ensure that the board of the directors are awareness of their information security duties
- Draft a comprehensive information security policy. Endorse the policy by senior management.
- Invest in hiring cyber security professionals to establish and manage a cyber security practice.

➔ Asset Management:

- Identify and classify all assets based on criticality and sensitivity
- Conduct periodic reviews to ensure the CMDB is accurate and up to date

➔ Third Part risk management:

- Create a process to identity and manage third party suppliers. The process should start by identifying suppliers, classifying suppliers, and conducting periodic security assessments on third party suppliers

➔ Cyber Security Risk Management:

- Create a process to assess and manage cyber security risks.
- The process should prioritise risks based on criticality and impact to the business.
- The process should be endorsed by the audit and risk committee and the current risk management team
- Create a cyber security risk register to document all cyber security risks
- Recommend an internal audit program to include cyber security in the scope

➔ Identity and Access Management:

- Implement and roll-out two factor authentication across the organisation as a priority
- Follow the principle of least privileges and separation of duties across the organisation
- Review admin users, eliminate sharing of admin passwords and implement a role based access control

- Conduct regular user access reviews to ensure that access management principles are consistently followed

➔ Security Education and Awareness:

- Employees should undergo security training at least once every 12 months
- Consider running simulated phishing attacks to further improve awareness

➔ Data Security and DLP:

- Undertake a data discovery activity. Classify and label data based on sensitivity and criticality.
- Utilise Microsoft Azure AIP to label data
- Consider implementing a DLP solution. A Microsoft DLP solution might be the best solution as the environment uses Microsoft products.
- Block USB flash drive usage. Only allow it (temporarily) when there is a business justification.

➔ Detection and Response:

- Invest in a SIEM solution. This could be using a Managed Security Service Provider (MSSP) or in house. Detecting cyber security incidents is a priority.
- Create an enterprise-wide cyber security incident response plan and at least 5 x cyber security incident response plans for the most common attack types.