Project Overhaul Oscorp Solution

Recommendations:
The following are a set of recommendations based on the NIST assessment that I conducted. The recommendations are prioritized in order of importance.

Key Areas of Improvements:

Cyber Security Governance:
• Hire a Cyber security manager or a Chief information security manager.
• Formalize cyber security roles and responsibilities. Ensure that the board of the directors are aware of their information security duties.
• Draw up 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 Party Risk Management:
• Create a process to identify 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 prioritize risks based on criticality and impact on 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 organization as a priority.

• Follow the principle of least privilege and separation of duties across the organization.
• Review admin users, eliminate sharing of admin passwords and implement a Role Based Access Control (RBAC).
• 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.
• Utilize 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 5X cyber security incident response plans for the most common attack types.