Risk Assessment Table:

Function	Category	Control ID	Description	Current State	Target State	Gap Summary	Recommended Actions	Priority	Status
Identify	Asset Management	ID.AM-1	Physical devices and systems are inventoried	Partial	Full	Inventory is incomplete and not centralized	Implement automated asset discovery; create unified CMDB	High	Open
Identify	Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented	Partial	Full	No formal vulnerability scanning process	Deploy monthly vulnerability scanning and reporting	High	In Progress
Protect	Access Control	PR.AC-1	Identities and credentials are managed for authorized devices and users	Partial	Full	Password standards weak; MFA not enforced	Enforce MFA, implement password policy, centralize IAM	High	Open
Protect	Data Security	PR.DS-1	Data-at-rest protection	Minimal	Full	Sensitive data stored without encryption	Enable full-disk encryption and encrypt sensitive storage folders	High	Open
Detect	Anomalies & Events	DE.AE-1	Baseline of network operations is established	Minimal	Partial	No formal monitoring baseline exists	Configure baseline in SIEM; monitor deviations	Medium	Not Started
Respond	Response Planning	RS.RP-1	Response plans are executed during or after an event	Partial	Full	IR plan exists but untested	Conduct tabletop exercises; update IR plan annually	Medium	In Progress
Recover	Recovery Planning	RC.RP-1	Recovery processes and procedures are executed	Partial	Full	Backups exist but recovery steps untested	Perform quarterly backup recovery testing	Medium	Open

NIST CSF Maturity Rating Guide:

Rating	Description
None	No controls in place
Minimal	Some informal or inconsistent controls exist
Partial	Controls exist but are incomplete or not standardized
Risk-Informed	Controls implemented based on organizational risk
Repeatable	Controls consistently followed and documented
Full	Control fully implemented, monitored, improved continuously

NIST CSF Compliance Gap Assessment — Executive Summary

This gap assessment evaluates Gladden Tech’s alignment with the NIST Cybersecurity Framework across the Identify, Protect, Detect, Respond, and Recover functions. The objective is to understand the organization’s current cybersecurity posture, identify gaps, and prioritize remediation actions.

Key Findings:

- Asset inventory and vulnerability management are only partially implemented.
- Access control maturity is low due to weak password standards and lack of MFA.
- Data encryption is not consistently applied, creating compliance and security exposure.
- Monitoring baselines and SIEM rules are underdeveloped.
- Incident Response and Recovery processes exist but require routine testing.

Overall Maturity Summary:

Function	Maturity
Identify	Partial
Protect	Partial
Detect	Minimal–Partial
Respond	Partial
Recover	Partial

Top 3 Recommended Priorities:

1. Implement MFA and strengthen password/identity policies.
2. Encrypt sensitive data at rest and enable full-disk encryption.
3. Deploy vulnerability scanning with scheduled reporting.

Conclusion:

Gladden Tech has foundational cybersecurity capabilities but requires improvement in access control, monitoring, and data protection to reach a fully mature, NIST-aligned posture.