NIST Cybersecurity Framework (CSF) 2.0 Mapping

Asset: kiranregmi.com
Owner: Kiran Regmi

GOVERN (GV) — Governance & Risk Oversight

Security ownership, objectives, and governance are formally defined. Security strategy and continuous review practices are documented.

IDENTIFY (ID) — Asset & Risk Awareness

Critical assets, realistic threat models, and internal risk assessments are documented to support informed decision-making.

PROTECT (PR) — Preventive Safeguards

Role-based access control, least-privilege design, and secure application architecture are implemented. Additional hardening is tracked via a remediation roadmap.

DETECT (DE) — Visibility & Anomaly Detection

Authentication and access events are logged. Enhancements for alerting and anomaly detection are planned as part of continuous improvement.

RESPOND (RS) — Incident Response

A structured incident response lifecycle is documented, including containment, investigation, recovery, and lessons learned.

RECOVER (RC) — Recovery & Resilience

Backup and recovery strategies are defined, with plans to formalize testing and automation.

CSF 2.0 Alignment Summary

CSF Function	Alignment Status	Notes
GOVERN	Strong	Ownership and governance defined
IDENTIFY	Strong	Assets and risks documented
PROTECT	Partial	Core controls implemented, hardening planned
DETECT	Partial	Logging exists, alerting roadmap defined
RESPOND	Strong	Incident handling documented
RECOVER	Partial	Backups defined, testing planned

This mapping demonstrates a risk-based, governance-driven approach to application security aligned with NIST CSF 2.0. Gaps are documented transparently and addressed through prioritized remediation.