Controls Shortlist (v0)

Project: Cybersecurity Program

Frameworks: NIST CSF, CIS Controls v8

Overview

This shortlist identifies key cybersecurity controls selected for a company, a 50-employee small-to-medium business with hybrid operations (HQ + branch + 20% remote).

The controls are chosen to provide balanced coverage of all five NIST CSF functions:

Identify (ID), Protect (PR), Detect (DE), Respond (RS), Recover (RC).

Project's resource constraints: CapEx ≤ $20k; OpEx ≤ $1.5k/month.

Identify (ID) — Understanding Assets and Risks

NIST ID	CIS v8 Control	Description	Implementation Status
ID.AM-1	1.1	Maintain inventory of hardware and virtual assets	✓ Implemented via centralized asset tracker
ID.AM-2	1.2	Maintain inventory of software and SaaS services	✓ Implemented using M365 Admin Center & SaaS management sheet
ID.RA-1	3.3	Conduct annual risk assessment	Planned using simplified NIST risk register
ID.GV-1	2.1	Establish cybersecurity governance and assign roles (RACI)	✓ Implemented — SOC Governance matrix

Protect (PR) — Safeguarding Assets and Data

NIST PR	CIS v8 Control	Description	Implementation Status
PR.AC-1	6.3	Enforce multi-factor authentication (MFA) for all users	✓ Implemented (M365 + VPN)

PR.AC-2	5.2	Apply strong password policy (length, complexity, expiration)	✓ Implemented
PR.DS-1	3.11	Encrypt data at rest and in transit	✓ Implemented (BitLocker, TLS)
PR.AT-1	14.1	Conduct annual security awareness and phishing training	✓ Implemented
PR.MA-1	7.5	Maintain system updates and patch management	✓ Implemented (WSUS / M365 Auto-Update)
PR.PT-1	4.6	Deploy endpoint protection (EDR/AV) across all devices	✓ Implemented — Defender for Endpoint
PR.DS-6	11.3	Ensure backup data immutability and offsite replication	Planned — via cloud backup vendor selection

Detect (DE) — Monitoring and Alerting

NIST DE	CIS v8 Control	Description	Implementation Status
DE.AE-1	8.1	Define baseline for network and user activity	✓ Implemented using SIEM log collection
DE.CM-1	8.2	Enable continuous monitoring (SOC/SIEM dashboards)	✓ In progress — Microsoft Sentinel setup
DE.DP-1	8.7	Centralize alert triage and escalation in ticketing system	Planned integration with Jira / Teams
DE.CM-8	8.11	Conduct regular phishing simulations and anomaly reviews	Planned quarterly

Respond (RS) — Incident Management and Communication

NIST RS	CIS v8 Control	Description Develop and maintain incident response plan	Implementation Status
RS.RP-1	17.1		✓ Implemented — see SOC Playbook

RS.CO-2	17.2	Define internal and external communication channels	✓ Implemented — via Teams and Email groups
RS.AN-1	17.3	Analyze incidents to determine root cause	✓ Ongoing process under SOC workflow
RS.MI-1	17.4	Contain and mitigate incidents based on runbooks	✓ Implemented — 4 runbooks developed
RS.IM-1	17.5	Document lessons learned and improvement actions	Planned — post-incident report template ready to use

Recover (RC) — Continuity and Resilience

NIST RC	CIS v8 Control	Description	Implementation Status
RC.RP-1	11.5	Develop and test recovery plan	Planned — to be tested Q1 2026
RC.IM-1	11.6	Conduct post-incident review to refine processes Communicate recovery status to stakeholders	Planned — integrated into SOC meetings
RC.CO-1	12.2		✓ Implemented — internal reporting template

Summary by NIST Function

Function	# of Controls	% Coverage	Implementation Progress
Identify (ID)	4	80%	Strong coverage
Protect (PR)	7	85%	Strong coverage
Detect (DE)	4	75%	Good coverage
Respond (RS)	5	80%	Good coverage
Recover (RC)	3	70%	To be expanded