**Basic Compliance Roadmap — SMB**

Hudson Valley CISO • Updated August 14, 2025

This roadmap gets me from ad‑hoc practices to a defensible, audit‑ready baseline aligned to NIST CSF and CIS Controls. Timelines assume a small team and prioritization alongside normal operations.

# Phase 0: Quick Wins (Weeks 1–2)

• Enforce MFA on email/SSO/admins • Patch criticals ≤7 days • Ensure EDR coverage • Verify backups + one restore test • Enable SPF/DKIM/DMARC

# Phase 1: Foundation (Days 15–45)

Policies: Acceptable Use, Password & MFA, Backup, Incident Response. Asset inventory, risk register, vendor list. Central logging for key systems. Define RPO/RTO for critical apps.

# Phase 2: Hardening & Visibility (Days 46–90)

Least-privilege RBAC, local admin reduction, MDM baseline, vulnerability scanning cadence, email security tuning, alert triage workflow. Awareness program launch.

# Phase 3: Audit-Ready (Days 91–150)

Metrics dashboard (MFA/patch/EDR/backup). Vendor due diligence with evidence. Tabletop exercise and after‑action improvements. Evidence repository for controls (tickets, screenshots, logs).

# Control Mapping (Starter)

NIST CSF: Identify (asset/risk/vendor), Protect (MFA, patching, backups, training), Detect (logging/alerts), Respond (IR plan), Recover (tested backups). CIS v8: 1–4 inventory and control basics; 5 Account Management; 6 Access Control; 7 Vulnerability Management; 10 Malware Defenses; 11 Data Recovery; 14 Security Awareness; 15 Service Provider Management.

# Evidence Checklist (Examples)

• MFA policy + console screenshots • Patch compliance report • EDR coverage report • Backup job status + restore logs • DMARC aggregate reports • Training completion logs • Vendor SOC 2/ISO certificates • IR contacts, tabletop notes