Summary

HCB (Hometown Community Bank), a (fictional) small financial institution, has completed a targeted mapping of 18 key CIS Controls Safeguards to the NIST Cybersecurity Framework 2.0 and its internal control catalog. This mapping supports GLBA compliance, PCI-DSS requirements, and a practical, risk-based security program tailored to the limited resources of a small bank.

The mapping is predominantly full strength, with one partial mapping (secure configuration baselines). Most controls are rated high priority and serve as foundational inputs for HCB's annual risk assessment.

Prioritized Controls & Risk Content

The table below summarizes the mapped controls, their HCB names, NIST CSF 2.0 references, and suggested priority based on risk-assessment impact.

# CIS ID	CIS Safeguard Title	HCB Control ID & Name	NIST CSF 2.0	Mapping Strength	Suggested Priority	Key Risk Application
1.1 / 1.2	Enterprise Asset Inventory	HCB-ID-001 Asset Inventory	ID.AM-01,02,05	Full	High	Foundational for ALL controls
2.1	Vulnerability Management + Automated Scans	HCB-PR-003 Patch & Vulnerability Mgmt	ID.RA-01,02 / PR.VM-01/02	Full	High	Prioritize remediation by risk score
3.1	Data Management Process	HCB-PR-004 + HCB-GLBA-001 Data Classification	PR.DS-01,02,05	Full	High	GLBA-mandated risk-based classification
5.1 / 5.3	Accounts Inventory + Disable Dormant	HCB-PR-001 Access Control & Account Inventory	PR.AC-01,04,07	Full	High	Risk-based privileged & dormant focus
6.1	Secure Configuration Process	HCB-PR-002 Secure Configuration Mgmt	PR.PS-01,02	Partial	High	Reduce misconfiguration risk (baseline first)
8.1	Enforce Multi-Factor Authentication	HCB-PR-001 MFA & Authentication Policy	PR.AC-01,06,07	Full	High	Apply to high-risk (privileged/remote) access
9.1	Ensure Use of DMARC / Email Protections	HCB-PR-007 Email Security & Anti-Phishing	PR.PS-01 / PR.AT-01	Full	Medium	Phishing risk reduction
10.1	Deploy & Maintain Anti-Malware	HCB-PR-006 Endpoint Protection	PR.PS-01 / DE.CM-04	Full	Medium-High	Standard endpoint baseline
11.1	Data Recovery Process + Automated Backups	HCB-RC-002 Backup & Data Recovery Mgmt	RC.RP-01,02 / PR.DS-04	Full	High	Ransomware / data-loss mitigation
13.1	Collect Audit Logs + Deploy SIEM	HCB-DE-001 Security Monitoring & SIEM	DE.CM-01,02,07	Full	High	Risk-based log collection & alerting
14.1	Security Awareness Training	HCB-PR-005 Security Awareness Training	GV.OC-03 / PR.AT-01,02	Full	Medium	Targeted training based on user risk
15.1	Vendor Management + Third-Party Risk	HCB-GOV-003 Third-Party / Vendor Risk Mgmt	GV.OC-02 / ID.RA-05 / PR.IP-01	Full	High	Dedicated vendor risk assessments required
16.1	Incident Response Plan	HCB-RS-001 Incident Response Plan	RS.RP-01,02 / RS.CO-01	Full	High	Risk-based scenarios & playbooks
17.1	Encrypt Data on End-User Devices	HCB-PR-004 Encryption & DLP	PR.DS-01,02	Full	High	Risk-based encryption decisions
18.1	Automated Pen Testing + Red Team	HCB-PCI-001 Penetration Testing & Red Team	ID.RA-03 / PR.VM-03 / RS.MA-01	Full	High	Scope & frequency driven by risk assessment
(Specific)	Information Security Program & Risk Assessment	HCB-GOV-001 InfoSec Program & Risk Assessmer	GV.OC-04 / GV.RM-03	Full/Direct	Critical	This IS the risk assessment control

Next Steps

Some steps that HCB should take from here.

- Complete the enterprise asset inventory (HCB-ID-001) by Q2 2026.
- Conduct the first formal risk assessment using HCB-GOV-001 to validate and refine priorities.
- Develop a 12-month implementation roadmap with assigned owners and budget.

Conclusion

HCB's security controls mapping provides a clear, standards-based roadmap that is both compliant and practical for a small bank. HCB is well-positioned to protect customer data, reduce cyber risk, and demonstrate strong governance.