IT Compliance Checklist
for Community Banks

Ensure your institution is ready for audits, secure against threats, and aligned with FFIEC/GLBA standards.

Security & Risk Management

- ☐ Multifactor authentication (MFA) is enforced for remote access
- ☐ Endpoint protection is active and monitored across all devices
- ☐ Regular vulnerability scans and penetration tests are conducted
- ☐ A documented incident response plan is in place
- ☐ Network segmentation is configured to protect sensitive data

Audit & Documentation

- ☐ You have up-to-date IT policies and procedures
- ☐ All vendor risk assessments are current and documented
- ☐ IT logs are retained and reviewed regularly
- ☐ Evidence of patch management and update is available
- ☐ Access controls are reviewed quarterly

Regulatory Readiness

- ☐ Systems are aligned with FFIEC Cybersecurity Assessment Tool (CAT
- ☐ Compliance with GLBA Safeguards Rule is documented
- ☐ Business continuity and disaster recovery plans are tested annually
- ☐ The board receives regular IT risk reports and status updates

Vendor Management

- ☐ Service providers have signed data protection agreements
- ☐ Critical IT vendors provide regular compliance evidence