

# Community Bank GLBA Readiness Checklist (Under \$300M in Assets)

## GOVERNANCE & ACCOUNTABILITY

- Designated Information Security Officer (internal or vISO)
- Board-approved Information Security Policy
- Documented cybersecurity oversight process
- Quarterly or semi-annual board reporting

## GLBA RISK ASSESSMENTS

- Annual IT risk assessment
- Cybersecurity risk assessment aligned to GLBA Safeguards Rule
- Documented remediation tracking
- Evidence of management review

## VENDOR & THIRD-PARTY RISK MANAGEMENT

- Vendor inventory with risk tiering
- Due diligence documentation for critical vendors
- Ongoing vendor monitoring process
- Contract review and regulatory alignment documentation

## ACCESS CONTROLS & SECURITY MEASURES

- Multi-factor authentication (MFA) implemented
- Role-based access control documented
- User provisioning & termination procedures
- Periodic access review evidence

## INCIDENT RESPONSE & TESTING

- Written incident response plan
- Documented tabletop testing
- Disaster recovery testing records
- Breach notification procedures



IF YOU IDENTIFIED GAPS IN ANY OF THESE AREAS, A STRUCTURED GLBA READINESS REVIEW MAY HELP PREVENT MATTERS REQUIRING ATTENTION (MRAS) DURING YOUR NEXT REGULATORY EXAM.