✅ The SMB Zero Trust Quick Start Checklist

Use this as a self-assessment or quick implementation guide.

🔐 Identity & Access Control

- ☐ Multi-factor authentication (MFA) is enabled across all systems
- ☐ No shared user accounts (especially for financial platforms)
- ☐ Role-based access enforced (least privilege model)
- ☐ Admin privileges are restricted and monitored

💻 Device & Endpoint Security

- ☐ All company devices are managed and monitored
- ☐ Endpoint detection and response (EDR) is deployed
- ☐ Outdated or non-compliant devices are blocked from access
- ☐ Patch management is automated

□ Application & API Security

- ☐ All third-party integrations are authenticated and reviewed
- ☐ API access is limited and monitored
- ☐ Sensitive systems are segmented from general access

👁 Monitoring & Visibility

- ☐ User activity logging is enabled across critical systems
- ☐ Alerts are configured for suspicious behavior
- ☐ Logs are retained for compliance and audit readiness

📊 Data Protection & Compliance

- ☐ Sensitive financial data is encrypted in transit and at rest
- ☐ Data access is restricted based on role and necessity
- ☐ Compliance requirements are mapped to security controls

▯ Employee Awareness & Governance

- ☐ Employees receive regular security training
- ☐ Acceptable use policies include AI and SaaS tools
- ☐ Shadow IT is actively monitored and managed

🏳 Scoring Insight

If you checked:

- ✅ 8–10 boxes: Strong foundation—focus on optimization
- ✅ 5–7 boxes: Moderate risk—prioritize gaps soon
- ✅ 0–4 boxes: High risk—immediate action recommended