✅ SMB Cybersecurity Compliance Checklist

1. Governance & Policies
- Define Information Security Policy (approved by management).
- Assign security owner / vCISO (internal or outsourced).
- Establish roles & responsibilities for IT, data, and incident response.
- Maintain asset inventory (systems, data, vendors).
- Review/update policies at least annually.

2. Access & Identity
- Enforce Multi-Factor Authentication (MFA) for all admin and email accounts.
- Implement least privilege and role-based access.
- Review user accounts quarterly; remove unused/terminated access.
- Maintain access logs (who accessed what, when).

3. Data Protection & Privacy
- Inventory and classify sensitive data (customer, employee, financial).
- Create a data flow map (where personal data is collected, processed, stored).
- Implement encryption in transit and at rest.
- Maintain a Data Retention & Disposal Policy.
- Publish/update Privacy Notice (GDPR/CPRA-compliant if applicable).
- Prepare DPIA (Data Protection Impact Assessment) for high-risk data.

4. Technical Security Controls
- Patch operating systems and applications regularly (document timelines).
- Deploy EDR/antivirus and monitor alerts.
- Enable centralized logging and log retention.
- Conduct regular vulnerability scans (internal + external).
- Restrict use of removable media and USB drives.

5. Incident Response & Business Continuity
- Document Incident Response Plan (who, what, when).
- Run at least one tabletop exercise annually.
- Maintain backup strategy (encrypted, offsite/cloud, tested quarterly).
- Document Disaster Recovery Plan (RTO/RPO objectives defined).

6. Vendor & Third-Party Risk
- Maintain vendor list (with services + data shared).
- Require security / compliance clauses in contracts.
- Review critical vendors annually (ask for SOC 2, ISO, or security questionnaire).
- Document risk ratings (low/medium/high) for vendors.

7. Compliance Evidence & Training
- Store all policies, logs, and security records in a central repository.
- Document security awareness training for employees (annual).
- Record phishing simulation or test results (if applicable).
- Keep incident logs (including near misses).
- Maintain audit readiness binder (evidence folder for frameworks).

8. Framework-Specific (as applicable)
- **ISO 27001**: Define ISMS scope, risk register, Statement of Applicability.
- **SOC 2**: Document control activities, monitoring, and evidence collection.
- **GDPR/Privacy Laws**: Record lawful basis for processing, DPIAs, and DSR (data subject rights) response process.
- **PCI DSS**: Segmentation, use of PCI-compliant payment gateways, annual SAQ.