in time tec

CREATING ABUNDANCE

SMB CYBERSECURITY READINESS CHECKLIST 2026

Your Quick Assessment Guide to Identify Security Gaps and Build a Resilient Foundation

Why this Checklist Matters ?

43% of cyberattacks target small businesses, yet only **14%** have a cybersecurity strategy. This checklist helps you assess your security posture across seven critical areas in just 15 minutes. Identify gaps, understand compliance needs, and prioritize security investments that protect your business.

 Vulnerability Assessment Status

- Have you conducted infrastructure vulnerability scans in the last 12 months?
- Do you maintain an inventory of all critical business assets and systems?
- Are high-severity vulnerabilities patched within 7 days of discovery?
- Have you completed a penetration test of critical systems in the last 24 months?
- Do you have a formal vulnerability management policy with defined remediation timelines?
- Is there documented evidence and reporting of all VAPT activities for audit purposes?

 Data Protection Compliance

- Have you documented all types of personal data your organization collects and processes?
- Is sensitive data encrypted both in transit (TLS/SSL) and at rest?
- Do you use data loss prevention (DLP) tools to prevent data exfiltration?
- Have you documented your lawful basis for collecting personal data (consent, contract, obligation)?
- Do you have data processing agreements (DPAs) with all third-party vendors handling personal data?
- Can you honor data subject rights including access requests, corrections, and deletion?

Cloud Security Posture

- Do you have a complete inventory of all SaaS applications in use?
- Is multi-factor authentication (MFA) enabled on all critical cloud platforms (email, file storage, financial systems)?
- Have you disabled public access to cloud databases, storage buckets, and sensitive resources?
- Are cloud storage permissions regularly audited for overly permissive access?
- Do you use role-based access control (RBAC) with the principle of least privilege?
- Are there centralized logging and monitoring of cloud activities and API calls?

Backup & Recovery Status

- Do you follow the 3-2-1 backup rule: three copies of two media types with one offsite?
- Are all critical business data and systems backed up daily or more frequently?
- Are backups encrypted and stored in immutable repositories (write-once storage)?
- Do you test backup restores at least quarterly to ensure data integrity?
- Have you defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical systems?
- Is the backup infrastructure isolated from production systems to prevent ransomware attacks?

Business Continuity Status

- Do you have a documented Business Continuity Plan identifying critical functions?
- Have you identified single points of failure (key personnel, critical systems, essential vendors)?
- Can employees work remotely with access to critical systems and data?
- Do you have a communication plan to notify employees, customers, and regulators during incidents?
- Are alternate systems or redundancy in place for critical applications?
- Is the Business Continuity Plan tested at least annually?

Endpoint Security & Remote Monitoring

- Do you have a complete inventory of all endpoints (laptops, desktops, servers, mobile devices)?
- Is antivirus or endpoint protection software actively running on all devices?
- Are security patches applied automatically and tested before deployment?
- Is full-disk encryption (BitLocker, FileVault) enabled on all laptops and portable devices?
- Do you have an RMM agent installed on systems to monitor health, performance, and security?
- Are endpoint threat detection and response (EDR) in place to identify suspicious activities?

People Security Management

- Have you conducted phishing simulation exercises for employees in the last 12 months?
- Is there a formal security awareness program covering phishing, social engineering, and reporting?
- Do employees have a one-click option to report suspicious emails integrated with your SOC or MSP?
- Are DMARC, SPF, and DKIM implemented to prevent email spoofing and BEC attacks?
- Is there a documented process to measure and improve user security behavior (click rates, report rates)?

Your Cybersecurity Readiness Score

Count your checkmarks across all seven sections:

Score Range	Readiness Level	Next Step
35–41 items	Mature	Continue monitoring; conduct annual reviews
27–34 items	Established	Address remaining gaps; schedule assessment
19–26 items	Developing	Implement critical controls in 90 days
Below 19 items	Foundation Stage	Establish foundational controls immediately

Priority Actions

Immediate (Next 30 Days)

- Enable Multi-Factor Authentication (MFA) on all critical systems prevents 99.9% of account compromise attacks.
- Verify backup systems with immutable, offsite backups and test recovery
- Conduct a vulnerability assessment of your IT infrastructure
- Inventory all endpoints and SaaS applications

Medium-term (30–90 Days)

- Deploy endpoint protection and remote monitoring (RMM)
- Implement data classification and encryption for sensitive data
- Develop a disaster recovery plan with defined RTO/RPO
- Conduct security awareness training for all employees

Get Your Personalized Security Assessment

Understanding where you stand is just the first step.
Close your security gaps with a professional assessment.

What You'll Receive

Detailed report scoring your security across all areas with specific vulnerability findings

Prioritized remediation roadmap based on risk level and business impact

DPDPA compliance alignment and regulatory guidance

Cost-effective security planning to optimize your investments

Ready to Secure Your Business?

Schedule Your Free 30-Minute Security Assessment Today

Learn where your security gaps are and get a customized roadmap to protect your business and comply with regulations. No obligation. No sales pitch. Just expert security guidance.

Three Steps to Secure Your Business

Schedule Assessment

Our security experts review your current controls and identify gaps

Get Your Report

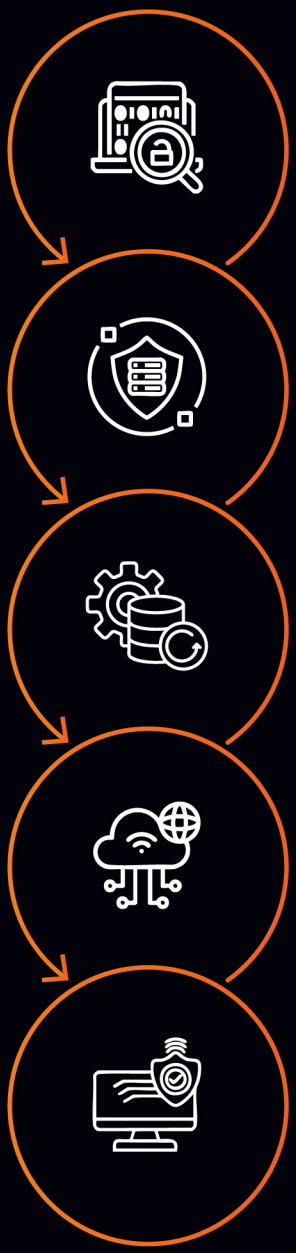
Comprehensive report with risk rankings and actionable recommendations

Implement Your Plan

We guide you through implementing critical controls from vulnerability fixes to disaster recovery

About In Time Tec

We specialize in helping 10–50 person SMBs build resilient security programs without complexity or enterprise costs. All services designed specifically for SMBs with flexible engagement models that fit your budget.



Vulnerability Assessment & Penetration Testing
Identify security weaknesses before attackers do

Data Protection & DPDPA Compliance
Implement compliant data protection controls and encryption

Disaster Recovery & Business Continuity
Build redundancy and recovery capabilities to minimize downtime

Cloud Infrastructure Security
Secure AWS, Azure, and SaaS environments with proper configuration and monitoring

Endpoint Security & Remote Monitoring
Deploy enterprise-grade endpoint protection and RMM tools

TALK TO OUR EXPERTS

Write us at: kuldeep.mathur@intimetecsoftware.com