ITVORTEX

SIMPLIFY. PROTECT. EVOLVE.

PREMIER BROADCOM VCSP PARTNER / VMWARE-POWERED CLOUD

SECURITY ASSESSMENT

IT Security Posture Checklist for SMBs.

Forty controls across eight critical domains, scored on a defensible rubric, with risk bands that map to real-world incident exposure. Know exactly where you stand and what to fix first.

40	8	4	30
CONTROLS	CRITICAL DOMAINS	RISK LEVELS	MINUTES TO SCORE

theitvortex.com
Paramus, NJ / 1 (844) 704-0684

Version 1.0
Security Assessment / 2026

WHY THIS CHECKLIST EXISTS

Most SMB breaches start with a control nobody got around to.

The hard part of SMB security is rarely the technology. It is keeping a defensible inventory of which controls are in place, which are partial, and which are missing. This checklist gives you a **repeatable 30-minute self-assessment** across the eight domains that drive insurance underwriting, audit posture, and real-world incident response.

43%

of all reported cyberattacks now target small and mid-sized businesses.

Verizon DBIR, multi-year average

$120K

median cost of a security incident for SMBs under 500 employees.

IBM Cost of a Data Breach, 2024

11 mo

average time SMBs take to fully recover operations after a ransomware event.

Industry benchmark

How to use this checklist

STEP 01

Score every control 0 to 3.

Use the rubric on page 7. Be honest. Partial credit exists for documented work in progress, but anything undocumented scores zero.

STEP 02

Sum your total out of 120.

Forty controls at a maximum of 3 points each. The risk bands on page 7 translate your total into a defensible posture statement.

STEP 03

Map zeros to a 90-day plan.

Every control scored zero becomes a remediation item. Prioritize by domain risk weight, not by how easy the fix is.

STEP 04

Re-score quarterly.

Posture decays. Re-run this checklist every quarter, share the trend with leadership, and tie improvement to cyber insurance renewal cycles.

THE 40-CONTROL CHECKLIST

Score every control. No fudging.

01. ENDPOINT PROTECTION

01	**EDR/XDR deployed on every endpoint** Not legacy AV. Behavioral detection and centralized response required.	☐
02	**All endpoints centrally managed** MDM or RMM enforces policy, patch state, and remote isolation capability.	☐
03	**Disk encryption enforced on every device** BitLocker, FileVault, or equivalent with key escrow to a managed location.	☐
04	**Local admin rights removed from daily-use accounts** Separate elevation account or JIT mechanism for admin tasks.	☐
05	**Removable media and USB controls enforced** Block, encrypt, or audit. No unmanaged data egress paths.	☐

02. PATCH MANAGEMENT

06	**Critical OS patches deployed within 14 days** Documented SLA per severity, with reporting and exception process.	☐
07	**Third-party application patching automated** Browsers, Adobe, Java, Zoom, Teams covered by the same tooling as the OS.	☐
08	**Firmware updates tracked for network and server gear** Firewalls, switches, hypervisors, iLO/iDRAC, storage controllers.	☐
09	**Vulnerability scanning runs at least monthly** Authenticated scans with remediation tickets and trend reporting.	☐
10	**End-of-life systems documented with sunset plan** Every unsupported OS, app, or appliance has a dated retirement plan.	☐

03. EMAIL SECURITY

11	**SPF, DKIM, and DMARC configured at quarantine or reject** DMARC at p=none is not implementation. Enforcement is required.	☐
12	**Advanced threat protection enabled** Sandbox detonation, URL rewriting, attachment scanning beyond signatures.	☐
13	**External sender warnings and impersonation detection active** First-contact warnings, display-name spoof detection, lookalike domain alerts.	☐
14	**Phishing simulation runs at least quarterly** Targeted scenarios, click and report rates trended, retraining for repeat clickers.	☐
15	**One-click phish report workflow for end users** Outlook or Gmail button that routes to a triaged inbox or SOC queue.	☐

04. IDENTITY & ACCESS

16	**MFA enforced on every account** Email, VPN, admin, all SaaS. Phishing-resistant methods preferred over SMS.	☐
17	**Privileged accounts separated from daily-use accounts** No admin email or web browsing on privileged credentials.	☐
18	**SSO consolidates major SaaS platforms** Entra ID, Okta, or equivalent for at least the top-10 business apps.	☐
19	**Offboarding revokes access within one business day** Documented checklist, HR-triggered, audited monthly.	☐
20	**Password policy aligned with NIST 800-63B** Length over complexity, breach-password screening, no forced rotation without cause.	☐

05. BACKUP & RECOVERY

21	**3-2-1 backup rule observed** Three copies, two different media, one offsite. Verified, not assumed.	☐
22	**Immutable or air-gapped backup copy exists** Ransomware cannot encrypt or delete the last line of defense.	☐
23	**Backup restores tested at least quarterly** Documented test plan, real workload restored, RTO measured, results signed off.	☐
24	**RTO and RPO documented per workload tier** Not one number for the whole estate. Tiered by criticality and revenue impact.	☐
25	**Backup encryption at rest and in transit** Keys managed separately from the backup admin role.	☐

06. NETWORK

26	**Next-gen firewall with active threat feeds** IPS, geo-blocking, application awareness, current subscriptions on every renewal.	☐
27	**Network segmentation across functional zones** Guest, corporate, IoT, server, OT separated with documented inter-zone rules.	☐
28	**Remote access via VPN or ZTNA only** Zero exposed RDP, zero exposed management interfaces.	☐
29	**DNS-layer filtering deployed** Blocks known-bad domains before TCP connection establishes.	☐
30	**Corporate Wi-Fi uses WPA3 or WPA2-Enterprise** Certificate or 802.1X auth. PSK is for the guest network only.	☐

07. MONITORING & RESPONSE

31	**SIEM or managed XDR aggregates logs from all critical systems** Identity, endpoint, firewall, cloud, email. Not one source in isolation.	☐
32	**Centralized log retention meets compliance window** Minimum 12 months for most frameworks. 7 years for some regulated workloads.	☐
33	**24x7 monitoring with named escalation contacts** In-house SOC, managed SOC, or MDR. Not "we'll check on Monday."	☐
34	**Incident response runbook documented and tested** Tabletop exercise at least annually. Contact lists, legal, insurance, PR included.	☐
35	**Time synchronization verified across all systems** Forensic correlation is impossible without consistent timestamps.	☐

08. GOVERNANCE & COMPLIANCE

36	**Cybersecurity insurance current with documented controls** Application answers match operational reality. Misstatement voids coverage.	☐
37	**Written information security policy reviewed annually** WISP, acceptable use, data handling, BYOD. Dated, signed, accessible.	☐
38	**Security awareness training annual for every user** Completion tracked, refresher on policy changes, role-specific modules for finance and execs.	☐
39	**Vendor risk assessment process documented** Critical vendors complete a security questionnaire and produce attestation reports.	☐
40	**Data classification and retention policies enforced** Confidential, internal, public tiers with handling rules and disposal timelines.	☐

SCORING RUBRIC

Score honestly. Compare to your peers.

Score each of the 40 controls on a 0 to 3 scale using the rubric below. Sum the totals to produce a posture score out of 120. Use the risk bands to translate that score into a defensible statement of your current exposure.

Per-control scoring scale

0
MISSING
Not implemented or no evidence exists.

1
PARTIAL
In place ad hoc, no documentation.

2
IN PROGRESS
Documented, partial coverage, on roadmap.

3
IMPLEMENTED
Documented, full coverage, evidence available.

Total score interpretation (out of 120)

100-120 — **Strong Posture**
Defensible across all eight domains. Maintain through quarterly re-scoring and tabletop exercises.

80-99 — **Moderate Posture**
Foundation is solid. Targeted gaps in two or three domains. Prioritize closing zeros within 90 days.

60-79 — **At Risk**
Material gaps. Insurance renewal will surface them. Build a structured 90-day remediation roadmap now.

< 60 — **Critical Exposure**
High likelihood of significant incident. Engage a managed security partner this quarter. Not next year.

Pro tip. Insurance carriers increasingly require evidence on roughly 20 of these 40 controls during renewal. A score under 80 will either raise your premium or limit your coverage. A score under 60 may trigger non-renewal entirely.

COMPLIMENTARY / 30 MINUTES

Validate your score with a security review.

Send us your completed checklist. Our security team will validate your scoring, flag the two or three controls we'd remediate first, and benchmark your posture against similar SMBs in your industry. No pitch, no obligation.

BOOK A POSTURE REVIEW

THEITVORTEX.COM

ABOUT IT VORTEX

IT Vortex is a Premier Broadcom VCSP Partner and VMware-powered managed cloud provider serving mid-market and enterprise clients. Our service portfolio spans cloud hosting (IaaS), desktop as a service (DaaS), disaster recovery (DRaaS), backup as a service (BaaS), and security as a service (SECaaS). We architect, build, and operate the infrastructure that runs our customers' most important workloads.

CONTACT

Phone	1 (844) 704-0684
Email	info@theitvortex.com
Web	theitvortex.com
Address	237 W Midland Ave Paramus, NJ 07652