# Where Your IT Stands Tonight

A 15-minute scorecard for Johannesburg and Gauteng business owners

**Complete it at your desk. You do not need a consultant to start.**

### WHO THIS IS FOR

SME owners and ops leads who pay the bills and want an honest picture of risk before something breaks.

### WHO THIS IS NOT FOR

Enterprises with a full-time security team, signed-off audits, and a live asset register you trust without asking anyone.

# How to use this

**Sit once. About 15 minutes. Honest answers.**

This is not a test you pass. It is a quick look under the hood. Most Johannesburg SMEs have never done it. Things mostly work until a laptop is stolen, ransomware hits, or a licensing bill lands that nobody expected.

Block out one quiet slot. Work through eight areas. Mark each area Green, Amber, or Red (scoring guide on the next page).

## Who should fill this in?

The owner or someone in ops who can make decisions. Not only the IT person. If one person holds all the passwords and never writes anything down, you need someone else in the room who can ask direct questions.

## What you need

1. About 15 minutes without interruptions
2. A pen (you will write on this page)
3. Access to ask one person who knows about backups, email admin, and who still has logins after staff leave

You do not need special tools. You do need honesty. "Probably fine" is how gaps stay hidden for years.

> On each area page, circle or tick one box:
>
> **G Green  A Amber  R Red**
>
> Definitions are on Page 3.

# How to score + what two reds means

**G**

**Green = fine for now**

You can see what you have. Basics are in place. No urgent gap you would be embarrassed to explain to a client or the Information Regulator tomorrow.

**A**

**Amber = needs attention this month**

Something is missing, outdated, or only half done. Not an emergency tonight, but it will become one if you ignore it.

**R**

**Red = urgent risk**

You cannot answer basic questions, or you know the answer is bad. Data, access, or continuity is at risk if something fails this week.

## Two or more reds = avoidable exposure

If two or more areas score Red, you are carrying real, avoidable exposure. That is the line from a proper first-pass audit: not panic, but a clear signal.

**Fix reds first.** Perfection is not the goal. Knowing where you stand is.

### Summary grid (write-on)

Fill in G, A, or R for each area as you go.

| # | Area | G | A | R |
|---|---|---|---|---|
| 1 | Assets | ◯ | ◯ | ◯ |
| 2 | Security basics | ◯ | ◯ | ◯ |
| 3 | Backups (and restores) | ◯ | ◯ | ◯ |
| 4 | Licensing | ◯ | ◯ | ◯ |
| 5 | Cloud / email | ◯ | ◯ | ◯ |
| 6 | Network / connectivity | ◯ | ◯ | ◯ |
| 7 | POPIA / personal data | ◯ | ◯ | ◯ |
| 8 | Documentation | ◯ | ◯ | ◯ |

**Total reds:** _____

# 1 Assets

**WHY THIS BITES**

You cannot secure or budget for what you cannot see. Most SMEs discover gaps only when something dies or walks out the door.

### What to look at

- [ ] 1. List every device: laptops, desktops, servers, phones, network gear.
- [ ] 2. Note who uses each device and whether it is company-owned or personal (BYOD).
- [ ] 3. Record approximate age and warranty status where you can.
- [ ] 4. Flag anything older than four to five years as a replacement risk.
- [ ] 5. If you have no list at all, stop here. That is your first finding.

**What "good" looks like**

A single list the business controls, updated when kit changes hands. You know what you own, who has it, and what is due for replacement. Finance and IT are not arguing from different spreadsheets.

**Score** ◯ G ◯ A ◯ R

**Who owns this?** _____

**If this is red, do this week**

- [ ] 1. Open a simple spreadsheet: device, user, age, warranty, location.
- [ ] 2. Walk the office (or ask each remote worker) and fill gaps in one sitting.
- [ ] 3. Mark anything 4+ years old for a budget conversation.
- [ ] 4. Store the list where the business controls it, not only on one person's laptop.

# 2 Security basics

**WHY THIS BITES**

Most SME breaches exploit basics, not exotic zero-days. Email and admin accounts are the usual door.

### What to look at

- [ ] 1. Endpoint protection on every device, not "Windows Defender is probably on."
- [ ] 2. Multi-factor authentication (MFA) enabled on email and any admin accounts.
- [ ] 3. Staff are not local administrators on their own machines.
- [ ] 4. A firewall exists and someone checks its logs occasionally.
- [ ] 5. You can name who is responsible when a security alert fires.

**What "good" looks like**

Every device has active protection. MFA is on for email and admin. Ordinary staff cannot install random software or disable security. Someone reviews firewall or security logs at least monthly.

**Score** ◯ G ◯ A ◯ R

**Who owns this?** _____

**If this is red, do this week**

- [ ] 1. Turn on MFA for all email and admin accounts today.
- [ ] 2. Remove local admin rights from standard user accounts.
- [ ] 3. Confirm antivirus or endpoint protection is running on each device (check the tray or management console).
- [ ] 4. Book 30 minutes to review firewall or security alerts from the last month.

# 3 Backups (and restores)

**WHY THIS BITES**

Backups that have never been test-restored are hope, not a plan. You find out at the worst moment.

### What to look at

- [ ] 1. What is backed up (files, email, servers, databases)?
- [ ] 2. How often backups run.
- [ ] 3. Where backups live: a second location or cloud, not only the same building.
- [ ] 4. When a restore was last tested, and whether it actually worked.
- [ ] 5. If load-shedding or a fire took out your office tonight, how many days of data would you lose?

### What "good" looks like

Backups run automatically on a schedule you can state without guessing. Copies sit offsite or in cloud. Someone restored a file or system in the last 90 days and it worked. You know the recovery time you can live with.

**Score** ◯ G ◯ A ◯ R

**Who owns this?** _____

### If this is red, do this week

- [ ] 1. Write down what is and is not backed up.
- [ ] 2. Confirm backups go to a second location (cloud or offsite), not only the office.
- [ ] 3. Restore one file and one larger item (mailbox or VM) and time how long it takes.
- [ ] 4. Fix whatever fails the test before you close the laptop.

# 4 Licensing

**WHY THIS BITES**

Unlicensed or over-deployed software is a compliance and audit risk. Forgotten subscriptions are pure waste.

### What to look at

- [ ] 1. List your key software (Microsoft 365, accounting, CAD, industry tools).
- [ ] 2. Note how each product is licensed (per user, per device, subscription).
- [ ] 3. Check counts: licences bought vs seats in use.
- [ ] 4. Record renewal dates so nothing auto-bills at a bad rate.
- [ ] 5. Flag subscriptions nobody uses but finance still pays.

**What "good" looks like**

A licence register matches reality. Renewals are in the calendar. No surprise true-up letters. You can answer "how many users?" without a three-day hunt.

**Score** ◯ G ◯ A ◯ R

**Who owns this?** _____

**If this is red, do this week**

- [ ] 1. Export active users from Microsoft 365 or Google Workspace and compare to paid seats.
- [ ] 2. List top five software bills and their renewal dates.
- [ ] 3. Cancel or downgrade unused subscriptions.
- [ ] 4. Store licence keys and contracts where the business controls them (see Area 8).

# 5 Cloud / email

**WHY THIS BITES**

Cloud sprawl and stale accounts are common, cheap-to-fix findings. Ex-staff with live logins are a data breach waiting to happen.

### What to look at

- [ ] 1. Where email lives (Microsoft 365, Google Workspace, on-prem, mixed).
- [ ] 2. Where file storage lives and who administers it.
- [ ] 3. Who has access to what (shared drives, admin portals, billing).
- [ ] 4. Whether ex-employees are fully deprovisioned (email, VPN, SaaS apps).
- [ ] 5. Whether anyone can name all cloud services the business pays for.

**What "good" looks like**

You know where mail and files live. Access follows job roles. Leavers are disabled the same day. No mystery admin accounts. One person can produce a list of cloud services in under ten minutes.

**Score** ◯ G ◯ A ◯ R

**Who owns this?** _____

**If this is red, do this week**

- [ ] 1. List active users in email and disable anyone who left in the last 90 days.
- [ ] 2. Review global admin / super-admin accounts; remove unknowns.
- [ ] 3. Write down every SaaS tool with a company login (even the small ones).
- [ ] 4. Turn on MFA if it is not already on (ties to Area 2).

# 6 Network / connectivity

**WHY THIS BITES**

One line, one router, no failover: the whole office stops when the ISP hiccups. In Johannesburg, load-shedding adds another cutover you did not plan for.

### What to look at

- [ ] 1. Business-grade connection with failover, or one line that takes everyone down when it drops.
- [ ] 2. Wi-Fi segmented: guests separate from business systems.
- [ ] 3. Critical gear (router, server, switches) on UPS or inverter backup.
- [ ] 4. Who to call when the line is down, and whether you have a backup (LTE, second ISP).
- [ ] 5. Whether remote staff can still work if the office loses power or connectivity.

### What "good" looks like

Internet fails over or restores without a full-day outage. Guest Wi-Fi cannot reach internal servers. UPS or inverter keeps core kit alive through load-shedding. You have tested what happens when power drops.

**Score** ◯ G ◯ A ◯ R

**Who owns this?** _____

### If this is red, do this week

- [ ] 1. Confirm which devices must stay up during load-shedding and put them on UPS or inverter.
- [ ] 2. Separate guest Wi-Fi from the business VLAN or SSID.
- [ ] 3. Write ISP account numbers and support numbers on paper (not only in email).
- [ ] 4. Test failover or LTE backup if you have it.

# 7 POPIA / personal data

**WHY THIS BITES**

If you hold names, emails, ID numbers, or any personal information about customers or staff, POPIA applies. You cannot protect data you have not mapped.

### What to look at

- [ ] 1. What personal information you hold (customers, staff, suppliers).
- [ ] 2. Where it lives: email, CRM, spreadsheets, cloud, paper files.
- [ ] 3. Who can access each store of data.
- [ ] 4. Whether ex-staff still have access to systems with personal data (links to Areas 5 and 2).
- [ ] 5. Whether your privacy notice matches what you actually do.

### What "good" looks like

A simple data inventory exists. Access is limited to people who need it. Leavers lose access promptly. You know who handles data subject requests. Security basics (MFA, backups, endpoint protection) are in place because POPIA expects reasonable safeguards.

**Further reading (not duplicated here)**

For the full POPIA walkthrough, see the live checklist: https://www.africanvanilla.co.za/blog/2026-08-popia-compliance-checklist-south-african-smes

*General guidance only, not legal advice.*

**Score** ◯ G ◯ A ◯ R

**Who owns this?** _____

### If this is red, do this week

- [ ] 1. Start a one-page data inventory: what you collect, where it sits, who can see it.
- [ ] 2. Disable access for anyone who left and still has system logins.
- [ ] 3. Check your privacy policy page is public and roughly matches reality.
- [ ] 4. Work through the POPIA checklist link above for the next gaps.

# 8 Documentation

WHY THIS BITES

If your IT person (internal or external) vanished tomorrow, could someone else pick up? Passwords in one head, vendor details in WhatsApp, and no diagram is how businesses stall for weeks.

**What to look at**

- [ ] 1. Passwords and admin credentials stored somewhere the business controls, not only in one person's memory.
- [ ] 2. Vendor contacts: ISP, hosting, software support, hardware supplier.
- [ ] 3. Network diagram or simple map: internet in, firewall, servers, Wi-Fi.
- [ ] 4. Licence records and renewal dates (links to Area 4).
- [ ] 5. Runbook or handover note: what to do first if email is down or ransomware hits.

**What "good" looks like**

A locked password vault or secure document the owner can open. Vendor list with account numbers. A sketch of the network a new tech could follow. You are not hostage to the one person who "just knows how it works."

**Score** ◯ G ◯ A ◯ R

**Who owns this?** _____

**If this is red, do this week**

- [ ] 1. Ask your IT person (or supplier) to document where passwords live and who has the master access.
- [ ] 2. Write down ISP, domain registrar, and Microsoft/Google admin contacts on paper.
- [ ] 3. Draw a one-page network sketch (boxes and arrows are fine).
- [ ] 4. Store copies where the owner can reach them if that person is on leave or leaves the business.

# Your picture + next step

Look at your summary grid on Page 3. Count the reds.

### 0 reds

Keep this paper. Re-score in 90 days or after a big change (new system, new office, staff churn).

### 1 red

Fix that one area this week. One focused sprint beats spreading attention across eight amber items.

### 2 or more reds

You are carrying real, avoidable exposure. Fix reds first, in order of what would hurt most if it failed tomorrow (usually backups, then access/security, then the rest).

**Perfection is not the goal. Knowing where you stand is.**

## Want a second pair of eyes?

African Vanilla offers a free IT audit for Johannesburg and Gauteng businesses. We run this checklist properly, then hand you a prioritised, no-obligation report.

**Book your free IT audit**

**africanvanilla.co.za/contact?intent=audit**

(Same eight-area framework online: africanvanilla.co.za/blog/2026-08-free-it-audit-checklist-johannesburg-smes)

AFRICAN VANILLA CONSULTING

**African Vanilla Consulting**

africanvanilla.co.za

+27 71 672 3800

5 Macanudo Street, Strauss Avenue, Wilgeheuwel, Roodepoort, Johannesburg, 1724