



WORKPLACE TECHNOLOGY | CONNECTIVITY | PRINT | SECURITY

SPECIAL REPORT

The SME Office Technology Health Check

What to review before you renew, replace or upgrade anything

Practical guide for South African SMEs

A business-focused article for owners, office managers and finance managers who need to review printers, phone systems, internet, Wi-Fi, security, cloud documents, support contracts and AI readiness as one working environment.

Prepared July 2026

Executive summary

For most SMEs, office technology has become one connected operating environment. Internet lines, Wi-Fi, hosted PBX, multifunction printers, cloud files, CCTV, access control, backup power and AI tools now depend on one another. Replacing one item in isolation can solve today's irritation while leaving the wider problem untouched.

The practical response is not to run a large technical project. It is to carry out a disciplined health check before the next renewal or replacement decision. That health check should connect business impact, cost, support accountability, security exposure and operational continuity.

- Review the office as one working environment rather than separate supplier contracts.
- Check connectivity, failover and support responsibility before judging VoIP, cloud, print or security systems.
- Include cybersecurity, access rights and business continuity in ordinary office-technology reviews.
- Treat AI as useful only where source documents, permissions and human review are controlled.
- Use a one-page decision record before signing a renewal or upgrade.

What this means for management: Before signing the next copier, phone, internet, CCTV or support renewal, the business should know what problem is being solved, what other systems are affected, what risk remains, who supports it, and how the decision will be reviewed later.

The SME Office Technology Health Check

What to review before you renew, replace or upgrade anything

Most office technology decisions start with a trigger: a copier contract is ending, the phone system is unreliable, the internet drops during calls, the Wi-Fi does not reach the boardroom, or a camera system no longer gives useful footage.

That is understandable. A business is busy. You normally look at the system that is causing pain today.

The problem is that office technology no longer works in separate boxes. A printer is not just a printer. It scans documents into workflows, stores data, connects to the network and may carry confidential information. A phone system is not just a PBX. It depends on internet quality, power, handsets, mobile users, cybersecurity and call routing. CCTV and access control are not separate either; they sit on the network, rely on storage and often touch personal information.

Before an SME renews, replaces or upgrades any one system, it is worth doing a simple office technology health check. The point is not to create a long technical project. The point is to see how the main systems support daily work, where they quietly create cost or risk, and what should be fixed before another contract is signed.

The practical test

Do not ask only whether a device still works. Ask whether it still supports the way the business now works.

1 Why replacing one item at a time can create bigger problems

Many SMEs make technology decisions in isolation because each supplier, device and contract has its own renewal date. This is how disconnected offices happen.

- A copier is replaced, but scanning still feeds a poor document process.
- A hosted PBX is installed, but internet failover and power backup are not considered.
- Wi-Fi access points are added, but nobody documents the network or guest access.
- CCTV is upgraded, but remote access permissions and retention rules are not reviewed.
- AI tools are introduced, but source documents, permissions and approval steps remain messy.

The business then owns newer equipment, but not necessarily a better working environment.

2 Start with business impact, not the product

A good health check begins with management questions. Which system causes the most interruptions? Which cost is rising without explanation? Where do staff create workarounds? Which process would hurt customers if it failed tomorrow morning?

Management question	What it usually reveals
Where do staff lose time every week?	Manual printing, poor scanning, unreliable calls, weak Wi-Fi, slow approvals or repeated supplier follow-ups.
Which failures stop trading?	Internet, phones, card machines, cloud files, access control, security systems or power-dependent devices.
Which costs are poorly understood?	Colour print, excess data, call charges, support exclusions, escalation clauses, licences or unused services.
Which risks are known but unmanaged?	Weak passwords, shared logins, missing backups, poor camera retention, old firmware or unclear data access.

3 Connectivity and failover: the foundation layer

Most modern office systems depend on reliable connectivity. Hosted PBX, cloud documents, remote support, card machines, email, scanning workflows, CCTV access and AI tools all suffer when the internet line is unstable or poorly supported.

The health check should confirm the primary internet line, backup route, router or firewall, Wi-Fi coverage, upload speed, support process and what happens during a power interruption. A cheap line can become expensive if it regularly breaks calls, delays work or leaves staff using mobile data to keep the business moving.

4 Hosted PBX and VoIP: more than cheaper calls

VoIP and hosted PBX decisions are often sold around call savings. Savings matter, but the bigger issue is continuity and customer experience. A phone system should route calls properly, support remote or mobile users, provide usable reporting and remain serviceable when the main internet line fails.

The review should include call quality, failover, handset age, mobile app use, voicemail, call recording, queue handling, Teams integration where relevant, and who is responsible when a problem crosses the phone platform, internet line, firewall and local network.

5 MFPs and managed print: look beyond the monthly rental

A multifunction printer is often treated as a rental line item. In practice, it can affect finance workflows, customer paperwork, HR files, scanning, secure print, data privacy and support time.

Before renewing a copier or MFP contract, review actual print volumes, colour usage, scan destinations, user controls, service response, device security, end-of-contract terms and whether the device still fits the way documents move through the business. The lowest monthly rental is not always the lowest-cost decision if the workflow remains slow or uncontrolled.

6 Wi-Fi, network and support: where small issues become daily frustration

Poor Wi-Fi is often accepted as normal office irritation. It should not be. Weak coverage, old cabling, unmanaged switches and undocumented network equipment can affect phones, printers, scanners, cloud software and security devices.

The health check should identify what equipment exists, who supports it, where it is documented, which devices connect to it and whether staff have a clear support route. A supplier cannot support what nobody can describe.

7 Cybersecurity: printers, phones and cameras are part of the risk

Cybersecurity is not only about laptops and email. Networked printers, VoIP systems, routers, Wi-Fi, CCTV, access control and cloud folders can all become weak points if permissions, passwords, updates and access controls are ignored.

For a practical SME review, start with basic controls: multi-factor authentication where available, strong admin passwords, named users rather than shared logins, current firmware, secure print for sensitive documents, backup checks, access reviews and a clear process for staff who suspect a phishing email or data issue.

8 CCTV, access control and power continuity

Security systems are often installed and then left alone until something happens. A useful review asks whether the cameras still cover the right areas, whether footage can be found quickly, how long recordings are retained, who has remote access and whether access control rights match current employees.

Power continuity should be reviewed at the same time. UPS units, backup power and restart procedures should protect the systems that keep the business operating: internet, phones, firewall, Wi-Fi, security devices and essential workstations. A backup system that is never tested is only an assumption.

9 AI readiness: useful only when the basics are under control

AI can help SMEs with summaries, document handling, customer responses, reporting, meeting notes and repeatable admin tasks. It does not fix poor source data, weak permissions or unclear workflows.

Before using AI in office processes, check whether documents are stored consistently, whether staff know which information may be used, whether outputs are reviewed by a responsible person and whether the business understands where customer or employee information is going. AI should support better work, not hide a broken process behind a polished answer.

10 Use a simple decision record before signing

A decision record is a one-page note that explains why management made a technology decision. It prevents future confusion and helps the next renewal start from facts, not memory.

Decision record field	What to capture
System or service	MFP, hosted PBX, fibre, LTE backup, Wi-Fi, CCTV, access control, cloud storage, backup or support.
Current problem	What is actually not working, costing too much or creating risk?
Business impact	Lost time, downtime, missed calls, security exposure, customer impact, cash cost or admin burden.
Options considered	Keep, repair, replace, consolidate, renegotiate, phase upgrade or defer.
Decision made	The selected option and why it is proportionate for the business now.
Dependencies	Internet, power, user training, firewall, software, licensing, support and contract timing.
Owner and review date	Who is responsible internally and when the decision should be reviewed.

11 Conclusion: do not upgrade blindly

Office technology does not need to be perfect. SMEs do not have unlimited time or budget, and not every old device needs to be replaced immediately.

But management should know which systems are stable, which systems create quiet cost, which carry security or continuity risk and which need attention before the next contract is signed.

The aim of an office technology health check is not to buy more technology. It is to make better decisions about the technology already carrying the business every day.

Final takeaway

Before replacing the next copier, phone system, internet line or security system, first understand the whole office environment. The cheapest quote is not always the lowest-cost decision, and the most advanced solution is not always the best fit.

One-page SME office technology health check

Use this checklist before a renewal, upgrade or supplier review. It is deliberately simple. The value lies in the management discussion it forces.

Area	What to check	R/A/G
Internet	Primary line, backup line, router/firewall, upload speed, reliability, support route	
Phones / VoIP	Call quality, routing, remote users, handsets, failover, recording, voicemail, reports	
MFP / print	Volumes, colour use, scan workflows, secure print, user controls, service response	
Wi-Fi / network	Coverage, cabling, switches, access points, guest network, documentation	
Cybersecurity	MFA, patching, endpoint protection, backups, admin rights, phishing awareness	
Cloud / documents	Folder structure, permissions, version control, retention, backup, data ownership	
CCTV / access control	Camera coverage, retention, access rights, maintenance, useful reporting	
Power continuity	UPS, backup power, runtime, testing, priority systems, restart procedure	
Contracts	End dates, escalation clauses, included support, variable charges, exit terms	
AI readiness	Clean data, repeatable workflows, privacy rules, human review, tool ownership	

How to use R/A/G

R/A/G means Red, Amber and Green. Green = working and proportionate. Amber = working, but with gaps or unclear ownership. Red = repeated failure, unmanaged risk, hidden cost or no continuity plan.

Suggested management discussion

- Which three issues cause the most daily frustration?
- Which system would hurt the business most if it failed tomorrow morning?
- Which supplier relationship is unclear or reactive?
- Which contract renewal is coming up in the next six months?
- Which process is still manual only because the current system makes change difficult?
- Which security risk is known but has not been assigned to anyone?