FREE CHECKLIST

SMB IT Planning Checklist

A year-ahead planning checklist that ties your technology decisions to your business plan.

INSIDE

7 planning areas · budget categories · a one-page annual roadmap · a review calendar

balancelogic.com · 301-396-8455

2026 edition

HOW TO USE THIS CHECKLIST

Most small and mid-sized businesses (SMBs) plan revenue, hiring and space a year ahead. Technology often gets planned one renewal notice or one failed laptop at a time.

This checklist walks you through an annual IT plan in seven areas, starting with the business and ending with a calendar. Work through it with the people who own the budget, operations and any outside IT providers. Tick what's done, note what isn't, and carry the gaps into the roadmap on the last pages.

Plan for a half-day working session to start, plus time to collect inventory and contract details beforehand. You don't need to finish every item in year one. A plan with five clear priorities is more useful than a list of fifty good intentions.

> **Tip:** bring last year's IT spending, your current contracts and your business plan to the first session. Planning without them turns into a wish list.

1. Business goals first

Every technology priority should trace back to something the business is trying to do. Start here, before anyone mentions a product.

- [ ] List the three to five business goals for the next 12 months (for example: open a second site, add a service line, win larger contracts, cut manual work).
- [ ] For each goal, write what technology it depends on or would change.
  A new service line may need new software, new data handling rules, or new skills.
- [ ] Name the business owner for each goal, not just the IT contact.
- [ ] Note any known events: office moves, lease ends, acquisitions, key retirements, new client requirements.
- [ ] Write down what frustrates staff most about today's technology. Ask them; don't guess.
- [ ] Agree on what "done" looks like at year end for each goal.

2. Technology priorities

Turn the goals into a short, ranked list of technology work. Each item needs a reason, an owner and a rough quarter.

- [ ] Translate each business goal into one or more technology projects.
- [ ] Add the "keep it healthy" work that doesn't tie to a goal but can't wait: end-of-support systems, expiring contracts, known security gaps.
- [ ] Rank the list by business impact and risk, not by which vendor called most recently.
- [ ] Mark projects that depend on each other (for example, a cloud move before a new phone system).
- [ ] Cap the year at what your team and providers can actually deliver alongside daily work.
  Overloaded plans quietly slip. Fewer finished projects beat many half-done ones.
- [ ] Record what you're choosing *not* to do this year, and why.

3. Inventory and lifecycle

You can't plan replacements for equipment and software you haven't listed.

What you have

- [ ] Computers, laptops, tablets and phones, with user, purchase date and warranty end.
- [ ] Servers, network equipment, firewalls and Wi-Fi access points, with age and support status.
- [ ] Printers, scanners, phones and other connected devices (cameras, door access, conference room gear).
- [ ] Software and cloud subscriptions, with license counts, owner and renewal date.
- [ ] Domains, websites, DNS and email services, with who holds the login.

What's coming due

- [ ] Flag every device or system that reaches end of vendor support in the next 18 months.
  Unsupported systems stop getting security updates. Plan the replacement before the deadline, not after.
- [ ] Set a standard replacement cycle for laptops and desktops and budget for it every year, not all at once.
- [ ] Check licenses for unused seats and duplicate tools that do the same job.
- [ ] Confirm the business, not an individual or a former provider, owns every admin account and domain.

4. Budget categories

Group spending so you can see where money goes and compare year to year. Fill in your own figures; the categories matter more than the totals at this stage.

Category	What belongs here	Last year	Next year
Hardware refresh	Planned replacement of computers, servers, network gear		
Software and subscriptions	Productivity suites, line-of-business apps, cloud services		
Managed services and support	Outside IT support, monitoring, help desk, internal IT staff time		
Security	Protection tools, backups, training, testing, insurance requirements		
Connectivity and phones	Internet circuits, backup connections, phone service		
Projects	One-time work from your priority list (moves, migrations, new systems)		
Compliance	Work driven by contracts, regulators or insurers		
Training	Staff skills on new and existing tools		
Contingency	Unplanned failures, urgent replacements, price increases		

- [ ] Separate one-time project costs from recurring costs so next year's baseline is clear.
- [ ] Check every recurring contract for renewal price increases before you finalize the budget.
- [ ] Agree who can approve unplanned spending, and up to what limit.

5. Security and compliance baseline

These are the basics to confirm every year. They don't replace a security assessment, but a "no" on any line belongs on your priority list.

- [ ] Multi-factor authentication is on for email, remote access, cloud apps and every admin account.
- [ ] Operating systems and applications get security updates on a set schedule, and someone checks that they installed.
- [ ] Business data is backed up, a copy is kept separate from the main systems, and a restore has been tested this year.
  A backup you haven't restored from is a hope, not a plan.
- [ ] Staff complete security awareness training and know how to report a suspicious message.
- [ ] Admin access is limited to the people who need it, and accounts are removed the day someone leaves.
- [ ] There's a written incident response plan with names and phone numbers, and it has been walked through.
- [ ] You know which rules apply to your data: contract clauses, industry regulations, state privacy laws and cyber insurance requirements.
- [ ] Your cyber insurance questionnaire answers match what's actually in place.
- [ ] Someone owns cybersecurity decisions at a leadership level, even if outside providers do the hands-on work.

Our work supports your compliance program. It doesn't guarantee compliance, certification, or assessment results.

6. Vendor and contract review

- [ ] List every technology vendor and provider: software, cloud, internet, phones, IT support, security, printers, website hosting.
- [ ] Record contract end dates, auto-renewal terms and notice periods on one calendar.
  Notice windows often close weeks or months before the renewal date. Miss one and you may be locked in for another term.
- [ ] Compare what each contract promises with what you actually received this year.
- [ ] Look for overlap: two tools or two providers doing the same job.
- [ ] Confirm who to call for what, and how each provider escalates problems.

- [ ] Check that each vendor's security practices meet the requirements your own clients and insurer place on you.
- [ ] Name one person who is accountable for how all your providers fit together.

7. People and training

- [ ] Write down who makes technology decisions today, formally and in practice.
- [ ] Identify skills gaps on the tools you already pay for. Underused software is a training problem as often as a software problem.
- [ ] Plan training for every new system in the roadmap, before go-live, not after.
- [ ] Document how new hires get set up and how leavers get removed, with a named owner for each step.
- [ ] Note any single points of knowledge: one person who knows the passwords, the vendor contacts or how a key system works.
- [ ] Decide whether you need more outside leadership or hands-on help this year, and for which areas.

Your one-page annual roadmap

Carry your top priorities from sections 1 to 7 into this table. Keep it to one page so it gets used.

Priority	Business goal it supports	Owner	Q1	Q2	Q3	Q4

Shade the quarter(s) when each priority is active. Mark dependencies with an arrow.

Review cadence

A plan only works if someone looks at it again. Put these on the calendar now.

When	What to review	Who
Monthly	Open issues, project progress, upcoming renewals, any security incidents	
Quarterly	Roadmap status, budget against plan, vendor performance, priorities for next quarter	
Twice a year	Backup restore test, access review (who has admin rights), incident response walk-through	
Annually	This full checklist, updated inventory, new budget, new roadmap	
When the business changes	New location, acquisition, major client requirement, key staff change	

Want help turning this into a plan?

A checklist shows you the gaps. Someone still has to own the plan. As a Managed Technology Provider, Balancelogic takes accountability for your technology function: aligning it with the business, setting priorities and coordinating the providers who do the work.

Book a free IT Strategy Session. Bring your completed checklist.

balancelogic.com/contact-us · 301-396-8455 · 3825 Leonardtown Road, Suite 5, Waldorf, MD 20601