ELEVATE
SOLUTIONS

WORKSHEET · IT STRATEGY & OPERATIONS

IT Budget Planning Worksheet 2026

Benchmarks by company size

Build a defensible IT budget: planning ranges by company size, a complete line-item worksheet, and a 3-year capital plan.

01 — PLANNING RANGES

IT spend planning ranges by company size

Before you fill in a single line item, you need an anchor: roughly what firms your size spend on IT, all-in, per person per month. The ranges below are the starting points we use in budget conversations.

> **READ THIS FIRST**
>
> These figures are planning guidance, not a survey, a benchmark study, or a third-party statistic. They are the ranges we use to open budget conversations with US small and mid-sized firms in 2026. Your number can legitimately land outside them. Use them to sanity-check your worksheet total — not to justify it.

"All-in" here means everything in the Section 02 worksheet: licensing, security tooling, support (internal or outsourced), connectivity, cloud, training, and an amortized share of hardware refresh. It excludes one-time projects such as an office move or a system migration — those belong in the contingency and capital sections.

HEADCOUNT BAND	PER-SEAT, MONTHLY (ALL-IN)	% OF REVENUE (PLANNING)	TYPICAL PATTERN
1–10 employees	$200 – $400	4% – 8%	Highest per-seat cost. Fixed costs (firewall, backup, security baseline) spread over few people.
11–25 employees	$175 – $350	3.5% – 7%	Per-seat cost starts to fall; first real spend on structured support and documentation.
26–50 employees	$160 – $320	3% – 6%	Security tooling matures (EDR, monitoring, awareness training); compliance costs appear as their own lines.
51–100 employees	$150 – $300	2.5% – 5.5%	Scale economies on licensing and support; co-managed or first internal IT hire common.
100+ employees	$135 – $275	2% – 5%	Lowest per-seat cost, but absolute spend is large enough to justify formal vendor management and annual review.

Planning ranges we use in budget conversations — guidance only, not a published benchmark.

What pushes you toward the high end

Two firms with identical headcount can sit at opposite ends of the same band. Expect to plan toward the top of your range if any of these apply:

- [ ] **You hold regulated data** 1
  PHI, client matter files, or financial records add security tooling, retention, assessments, and insurance-driven controls that lightly regulated firms skip.
- [ ] **Downtime is expensive for you** 2
  If billable hours, patient schedules, or trading windows stop when systems stop, you pay for redundancy: backup circuits, tighter recovery targets, tested failover.
- [ ] **Hybrid or distributed work** 3
  Every remote seat needs the same security posture as an office seat — device management, identity protection, and secure remote access all carry per-seat cost.
- [ ] **Aging estate** 4
  Deferred refresh shows up later as a spike. If most hardware is past year three, plan high for the next two cycles.
- [ ] **Audit, litigation, or carrier scrutiny** 5
  Cyber insurance applications, client security questionnaires, and regulator exams all generate work and tooling requirements that belong in the budget, not in a scramble.

CONTEXT FOR THE SPEND

Security lines are usually the first target in a budget cut and the most expensive to get wrong. The US average cost of a data breach reached $10.22M — a record high. IBM Cost of a Data Breach Report 2025 For organizations under 500 employees, the last published by-size average was $3.31M per breach. IBM Cost of a Data Breach Report 2023 Keep those numbers in mind when Section 02's security category looks large.

02 — LINE ITEMS

The line-item worksheet

Sixty-four line items across eight categories. Work through every row: enter a monthly figure, an annual figure, or both, and write "$0 — confirmed" rather than leaving a row blank. The rows you skip are the ones that surprise you in Q3.

Pull last year's actuals from your accounting system and your card statements first — SaaS sprawl hides on corporate cards. Where a cost is annual (insurance, assessments, refresh), divide by twelve for the monthly column so the per-seat math in Section 01 works.

Category A — Hardware (10 line items)

ITEM	MONTHLY $	ANNUAL $	NOTES
Laptops & desktops — refresh plus new hires			
Monitors, docks & peripherals			
Mobile devices (phones, tablets)			
Printers, scanners & multifunction devices			
Conference room AV & video equipment			
Servers & on-premises hosts			
Storage hardware / NAS			
UPS & power protection (incl. battery replacement)			
Spares & loaner pool			
Hardware warranties & extended support			
Subtotal — Hardware			

Category B — Software & SaaS (10 line items)

ITEM	MONTHLY $	ANNUAL $	NOTES
Microsoft 365 / Google Workspace licenses			
Line-of-business application (practice mgmt, EHR, portfolio)			
Document management system			
Accounting, billing & time-capture software			
CRM / client intake platform			

E-signature platform			
PDF & document tools (Adobe or equivalent)			
Password manager (business tier)			
Project & collaboration tools			
Other departmental SaaS (inventory from card statements)			
Subtotal — Software & SaaS			

Category C — Security (10 line items)

ITEM	MONTHLY $	ANNUAL $	NOTES
Endpoint detection & response (EDR)			
24/7 monitoring / managed detection & response			
Email security (advanced filtering, phishing & BEC protection)			
Security awareness training & phishing simulation			
Identity protection / MFA licensing uplift			
Vulnerability scanning & patch management tooling			
SIEM / security log retention			
Encryption & data loss prevention tooling			
Penetration test / security assessment (annual)			
Cyber insurance premium			
Subtotal — Security			

Category D — Network & infrastructure (8 line items)

ITEM	MONTHLY $	ANNUAL $	NOTES
Primary internet circuit			
Backup internet circuit (failover)			
Firewall hardware & security subscriptions			
Switches & wireless access points			
Remote access (VPN / zero-trust access)			
Phone system / VoIP service			
Cabling, racks & physical infrastructure			
Domains, DNS & certificates			
Subtotal — Network & infrastructure			

Category E — Cloud (6 line items)

ITEM	MONTHLY $	ANNUAL $	NOTES
Cloud compute & storage (Azure / AWS / other)			
Backup — servers & endpoints			
Backup — Microsoft 365 / SaaS data			
File storage & sync (SharePoint, cloud file server)			
Disaster recovery replication / DRaaS			
Cloud overage buffer (egress, storage growth)			
Subtotal — Cloud			

Category F — Support & services (8 line items)

ITEM	MONTHLY $	ANNUAL $	NOTES
Managed IT services agreement			
Out-of-scope / per-incident support			
Internal IT salaries & benefits			
Specialist consulting (architecture, compliance, projects)			
Vendor support & maintenance contracts			
Onboarding / offboarding service fees			
After-hours & emergency support			
IT documentation & asset management tooling			
Subtotal — Support & services			

Category G — Training & compliance (6 line items)

ITEM	MONTHLY $	ANNUAL $	NOTES
Compliance assessments (HIPAA, SOC 2, client audits)			
Compliance / GRC software			
Staff technology training (beyond awareness platform)			
IT staff certifications & continuing education			
Policy development & review (counsel or consultant time)			
Audit & e-discovery readiness (retention, legal hold tooling)			
Subtotal — Training & compliance			

Category H — Contingency & projects (6 line items)

ITEM	MONTHLY $	ANNUAL $	NOTES
Planned projects — this year (list each in notes)			
Office move / expansion IT costs			
Emergency hardware replacement reserve			
Incident response retainer / breach response reserve			
Renewal price-increase buffer (most SaaS renews upward)			
General contingency (a 5%–10% hold-back is the planning range we use)			
Subtotal — Contingency & projects			

ROLL-UP	MONTHLY $	ANNUAL $	÷ HEADCOUNT = PER-SEAT
TOTAL — all eight categories			

Divide the monthly total by headcount and compare against your band in Section 01. If you are far below the low end, the usual cause is not efficiency — it is missing rows: backup, security monitoring, training, or contingency at zero.

03 — CAPITAL PLAN

3-year capital planning

Hardware fails on a schedule whether you budget for it or not. A 3-year staggered plan turns refresh from a surprise capital hit into a flat, predictable line.

Refresh cycles we plan against

ASSET CLASS	REFRESH CYCLE (PLANNING)	NOTES
Laptops	3–4 years	Battery wear, warranty expiry, and OS support windows converge around year four. Heavy travelers trend toward three.
Desktops	4–5 years	Longer life than laptops; refresh with the OS support window, not the chassis.
Servers	5 years	Plan the replace-vs-migrate-to-cloud decision at year four, not year five.
Network gear	5–7 years	Firewalls earlier (security subscriptions track hardware generations); switches and access points later.
Phones	4 years	Driven by vendor security-update windows more than by hardware failure.
UPS batteries	3–4 years	The component everyone forgets. A UPS with a dead battery is a power strip.

Planning ranges we use — adjust for your usage profile and vendor support windows.

> **END-OF-LIFE IS A COMPLIANCE PROBLEM, NOT JUST AN IT PROBLEM**
>
> An operating system or device past its vendor's end of support stops receiving security patches. Windows 10 is already past end of support. Running unsupported systems can put you out of step with cyber insurance application answers, HIPAA Security Rule expectations around patching, and client security questionnaires — and a known-unpatched system is a difficult fact to defend after an incident. Treat vendor end-of-support dates as hard deadlines in this plan.

Staggered refresh worksheet

Inventory each asset class, then spread replacement across three years — oldest and highest-risk first. Aim to replace roughly a third of each fleet per year so no single year doubles your hardware line.

ASSET CLASS	UNITS TOTAL	YEAR 1 (#/$)	YEAR 2 (#/$)	YEAR 3 (#/$)
Laptops				

Desktops				
Servers / hosts				
Firewalls				
Switches & access points				
Phones / mobile				
UPS units / batteries				
Capital total per year				

Plan owner _____

Next review date _____

04 — BUDGET DEFENSE

The budget defense template

A budget survives the CFO conversation when every line answers one of three questions: what risk does it avoid, what obligation does it meet, or what capability does it buy. A line that answers none of them deserves to be cut.

One page, four parts

- [ ] **1. The headline number, in business terms** 1
  Total annual spend, per-seat monthly, and the Section 01 band you fall in. One sentence on what moved versus last year and why.
- [ ] **2. Every major line tied to a justification** 2
  For each category subtotal: risk avoided (e.g., backup → ransomware recovery), obligation met (e.g., compliance assessment → client contract or regulation), or capability gained (e.g., refresh → fewer hours lost to slow machines).
- [ ] **3. The cost of the alternative** 3
  Your downtime number (formula below) and the relevant breach context. The human element is involved in 60% of breaches Verizon DBIR 2025 — which is the business case for the training line, in one clause.
- [ ] **4. What you would cut first, and what you will not** 4
  Showing the priority tiers below signals you have already done the discipline the CFO would otherwise impose.

Cost-of-downtime formula

One defensible number beats ten adjectives. Compute the hourly cost of a systems outage:

> **HOURLY DOWNTIME COST**
> (Annual revenue ÷ annual working hours × % of revenue that stops when systems stop) + (affected employees × average loaded hourly cost × % productivity lost) + direct recovery costs per hour. Label the result an internal estimate and show your inputs.

INPUT	YOUR FIGURE	SOURCE / ASSUMPTION
Annual revenue ÷ annual working hours		
% of revenue dependent on systems		
Affected employees × loaded hourly cost		
% productivity lost during outage		
Direct recovery cost per hour		
Estimated hourly downtime cost		

How to cut safely when you must

Budgets get trimmed. The discipline is cutting in the right order. Deferring a hardware refresh by six months is a managed risk you can document. Cutting backup, monitoring, or training is a different category of decision: it removes the controls that determine what an incident costs. Breaches contained in under 200 days averaged $3.61M versus $5.49M for those that ran longer IBM Cost of a Data Breach Report 2025 — containment speed is bought with exactly the tooling that looks optional on a spreadsheet. Deferring refresh is not the same as cutting security; never present them as interchangeable.

Priority tiers (fill in your own lines)

TIER	DEFINITION	YOUR LINES
Tier 1 — Protect	Cut last, restore first: backup and recovery, security monitoring, identity protection, compliance obligations under contract or regulation.	
Tier 2 — Defer with a date	Can slip one or two quarters with documented risk and a firm new date: hardware refresh, planned projects, office buildout.	
Tier 3 — Discretionary	Cut first if needed: convenience tooling, duplicate SaaS, upgrades without a risk or obligation attached.	

Budget approved by _____

Date _____

Elevate Solutions

6230 Wilshire Blvd Suite 2120, Los Angeles CA 90048

(424) 400-6625 · support@elevatesolutions.io · elevatesolutions.io