LERNER SOLUTIONS

IT PLAYBOOK FOR SERIES A STARTUPS

Your Field Guide to Scalable IT



v1.2 Sept. 2025



What's Inside?

01 Setting the Stage 3

The Big Picture 4
How To Use This Field Guide 6
The IT Scaling Traps 7

02 Functional Deep Dives 8

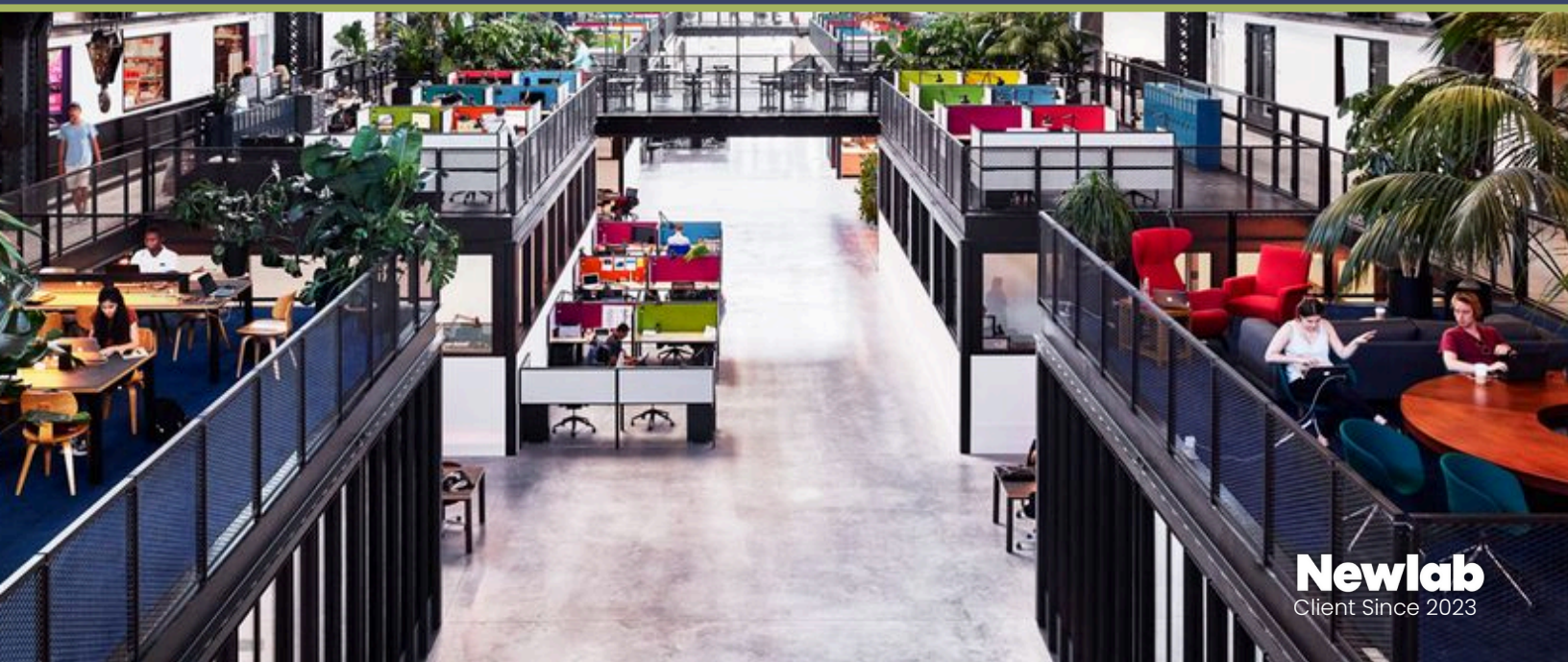
Identity & Access 9
Devices & MDM 11
Security 13
Networking 15
Data & SaaS Governance 16
Workforce Enablement 18
Policies, Procedures & Docs 20

03 Quick References 22

One-Page Cheat Sheet 23
Compliance Checklist 24
Budget Benchmarks 25
Staffing Models 26
Recommended IT Stack 27
IT Health Check 28
Jobs to Be Done 29

01
SETTING THE STAGE

The Big Picture
How To Use This Field Guide
The IT Scaling Traps



THE BIG PICTURE



Here are our 6 foundational pillars that are the difference between building a scalable IT framework and building a pile of tech debt that will crumble under the weight of your company's growth.

01 Invest Some Now, or Invest More Later

Every technical decision is a choice: invest time now for a scalable solution, or take a shortcut that creates “tech debt” you’ll repay later. Prioritizing a solid foundation prevents the costly rework and security crises caused by temporary fixes.

02 Standardize & Simplify

Perfection is impossible at Series A, and complexity is the enemy of scale. Work in incremental steps, but always plan ahead of the curve by standardizing on a minimal set of high-quality tools and processes that can evolve without major rewrites.

03 Trust is Earned, Not Given

In a company with no perimeter, trust is a privilege, not a default. This Zero Trust foundation means we continuously verify every user and device, forcing us to build intentional, secure systems instead of relying on a broken, trusted network.

04 IT as a Force Multiplier

IT's role isn't to say "no," but to build IT systems that make everyone else more effective. Every automation and self-service tool should eliminate friction and be designed to multiply the productivity and velocity of your colleagues.

05 Prioritize Employee Experience

In the competition for talent, the quality of an employee's tools is a competitive advantage. From unboxing a laptop to daily software use, the IT experience must be seamless and empowering to drive productivity, morale, and retention.

06 Everything Must Be Observable

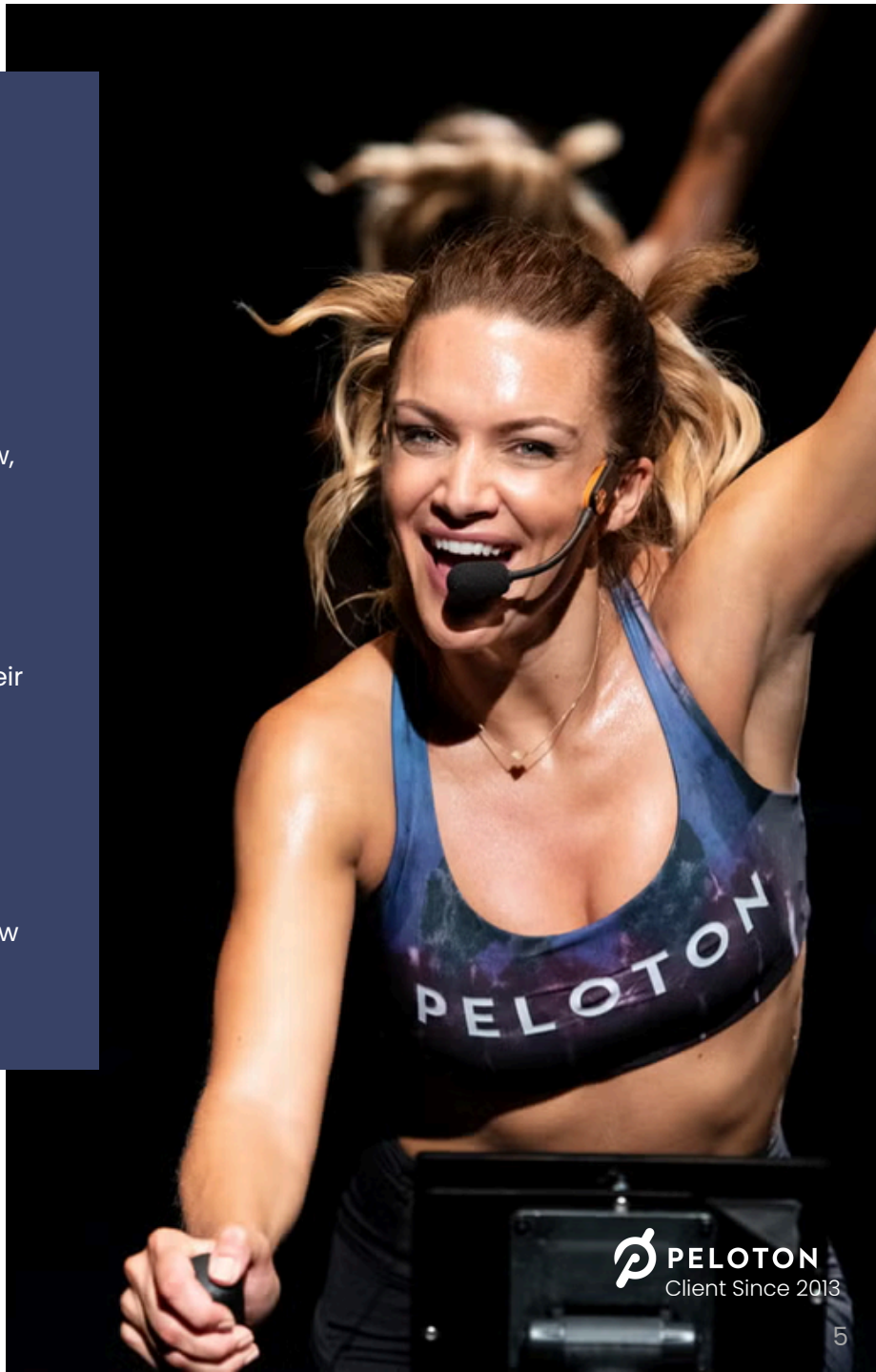
You cannot manage or secure what you cannot see, and manual inspection is impossible at scale. Every system must be built to be observable, generating the logs and metrics needed to understand its health and prove compliance.

IT Gut Check

The Onboarding Test
If we hired 10 people to start tomorrow, would it be a seamless, impressive experience or a chaotic fire drill?

The Offboarding Test
If our most senior engineer resigned right now, could we revoke 100% of their access to everything in under 10 minutes?

The Big Customer Test
If a Fortune 500 prospect asked for proof of our security controls today, would we be ready to pass their review and close the deal?



PELOTON
Client Since 2013

HOW TO USE THIS FIELD GUIDE

If You Want to Focus On . . .	Then Read . . .
Strategy & Big Picture	Read **The Big Picture** to grasp the 'why.' Read the **TL;DR boxes** in the Functional Deep Dives to get the 'what.' Review the **One-Page Cheat Sheet** and **Budget Benchmarks** to understand the roadmap.
Build Technical Foundation	Start with the **IT Health Check** to diagnose your gaps. Then, execute on the "big three" deep dives: **Identity**, **Devices**, and **Security**.
Specific Project Need	Jump directly to the relevant **Functional Deep Dives** (e.g., Networking, Security) or **Quick References** (e.g., Tool Recommendations, Jobs to Be Done)
Planning & Roadmap	Use the **One-Page Cheat Sheet** to illustrate the path, and the **Budget Benchmarks** and **Staffing Models** to build your financial case.
Just Browsing the Content	Take a few minutes to flip through it all, but head to **Quick References** for ready-to-use content without needing to read a full chapter.



THE IT SCALING TRAPS

Early on, speed is survival, and many intuitive shortcuts feel like the right move. But these shortcuts are well-disguised traps that create chaos and hold back growth.

01 The Grow-at-All-Costs Blindspot

The Trap: "Anything that doesn't directly build product or close deals is a distraction. We must focus 100% of our resources on growth; foundational IT and security are cost centers to be minimized."

The Reality: This mindset treats the core systems that enable productivity and security as blockers, not accelerators. By underinvesting, you create a drag on the entire organization, leading to a slower, less secure, and more chaotic company that ultimately can't sustain the growth you're chasing.

02 The Reactive IT Culture

The Trap: "We empower our teams to choose their own tools, and our IT team is great because they are super responsive to every request. This agility is our strength."

The Reality: This reactive culture, driven by decentralized decisions, forces IT into a constant firefighting mode. While daily tickets get closed, no foundational work is done on automation or security. The company accumulates massive operational debt, becoming brittle and unable to support the next stage of growth. This is where partnering with a compliance-savvy MSP can de-risk the sales process.

03 The "Checkbox" Security Plan

The Trap: "We're secure enough for now. We have MFA, EDR, and backups in place, and we just passed our first big customer's security review."

The Reality: This "checkbox security" creates a false sense of security while ignoring the harder work of data governance, vendor risk management, and tested incident response. When a major enterprise customer requires a certification like SOC 2, you're faced with a nine-month scramble after discovering your toolset was only 20% of the solution.

02

FUNCTIONAL DEEP DIVES

Identity & Access
Devices & MDM
Security
Networking
Data & SaaS Governance
Workforce Enablement
Policies, Procedures & Docs



Client Since 2021

IDENTITY & ACCESS

TL;DR Enforce SSO and MFA from the start, and automate account lifecycle to prevent orphaned accounts, reduce onboarding delays, minimize offboarding mistakes, and keep access consistent, secure, and audit-ready as you scale.

The Central Nervous System

If you only get one thing right, make it identity. Your identity platform is the central nervous system of your entire company—it controls who has access to what, when, and from where. Getting this foundation correct is the single most important driver of both security and employee productivity. A well-run identity stack makes onboarding seamless and offboarding instant.

If your internal team is light on identity expertise, partnering with an MSP like Lerner Solutoins ensures you avoid misconfigurations that create security gaps.

The Non-Negotiables: SSO & MFA

- **Multi-Factor Authentication (MFA):** Enforce on all critical systems. Authenticator apps are a solid baseline, but stronger methods exist — like adaptive MFA (e.g., Okta) — that validate identity with multiple factors and reduce phishing risk.

- **Single Sign-On (SSO):** If budget & scale allow for it, then mandate that every new business-critical application must support SAML or OIDC for SSO. This is a productivity feature (one less password) and a critical security control (one place to sever all access).

Tool Recommendations

Category	Tool	When to Choose	Why It Matters
Directory & IdP (Includes core SSO, MFA, & Lifecycle features)	Okta	From the start if budget allows; otherwise layer in as app count grows beyond 10–15	Central nervous system of identity; automates provisioning & deprovisioning, enforces MFA, and scales with your SaaS stack.
Privileged Access Management (PAM)	Keeper	From the start for password management. Then expand use once engineers need access to critical infrastructure (AWS, DBs, production systems)	Provides auditable, time-bound access; avoids shared admin logins

Your Auditor's Wishlist: A Sample Evidence Request

The full evidence request list for a SOC 2 audit can have over 100 items. Below is a sample of the most common and critical artifacts your auditor will ask for. Importantly, having a policy on paper is not enough. You must also produce evidence that the policy is being followed in practice.

- Your version-controlled Information Security Policy and annual Risk Assessment.
- Evidence of the full user lifecycle: MFA enforcement, access reviews, and timely deprovisioning.
- A complete system inventory and a current network and data flow diagram.
- MDM and EDR reports showing 100% agent deployment and fleet-wide compliance.
- Evidence of a continuous vulnerability management process for all external-facing systems.
- Sample change management tickets showing your formal review, testing, and approval process.
- Security awareness training completion reports and your annually tested Incident Response plan.

What We See Go Wrong

Delayed SSO Adoption

Waiting until you have 50+ apps to enforce SSO. This creates a massive, painful cleanup project and leaves dozens of insecure, unmanaged login points.

Optional MFA

Making MFA "opt-in" for employees. Adoption will be low, and it gives a false sense of security. It must be enforced.

Slow, Manual Offboarding

Relying on a manual checklist to deactivate accounts when someone leaves. Inevitably, accounts are missed, leaving ex-employees with access to company data for weeks or months.

Unmanaged SaaS Sprawl

Letting employees subscribe to apps freely, which creates a costly and insecure environment where data is unaccounted for and offboarding consistently fails.



GAMES
Client Since 2022

DEVICES & MDM

TL;DR Centrally manage all laptops with an MDM. Enforce a hardened security baseline, use zero or near zero-touch provisioning, immediate & complete access revocation for offboarding, and keep a spare pool on hand to drastically reduce employee downtime.

The Fleet is Your Responsibility

An employee's work laptop is a critical company asset and an extension of your corporate environment. Allowing *unmanaged* personal devices (BYOD) for full-time employees is a security and compliance nightmare you cannot afford. You must own and manage the fleet. As you scale, if you end up having both Macs and PCs, then it's critical to plan for that mixed fleet from the beginning.

MDM: Foundational Control Layer

A Mobile Device Management (MDM) solution is the foundation for controlling your laptop fleet. Two critical functions:

- **Automated Provisioning:** Zero-touch or near zero-touch deployment powered by Jamf (macOS) and Ninja (Windows) lets you ship factory-sealed laptops that auto-enroll and configure on first boot without IT touching the box.
- **Continuous Management:** More importantly, MDM provides ongoing control: enforce security baselines (encryption, passwords), patch OS/apps, and remotely lock or wipe lost devices.

What We See Go Wrong

Delayed MDM
Waiting until you have 50+ "wild" laptops in the fleet. The pain of retroactively enrolling devices from busy employees is immense. You must start from device #1.

Offboarding Oversights
Failing to immediately & completely revoke departing employee's access. Every hour that their email, file shares, and SaaS accounts remain active past their departure is a significant security and data exfiltration risk.

No Standardization
Allowing teams to buy dozens of different makes and models. This makes support, security baselining, and maintaining a useful spares pool impossible to manage at scale.

Improper Spare Pool
Having too few or many replacement laptops ready to ship. Too few leads to delays and poor productivity. Too many is a poor investment and provides additional entry points for bad actors.

Zero- or near-zero touch deployment is straightforward at 20 laptops, but at 200 it's a different story. Working with an MSP like Lerner can save weeks by automating the setup and logistics

Your Day One Security Baseline

Your MDM is the tool you use to turn policy into reality. It should enforce a minimum set of security controls on every corporate device, with no exceptions:

- **Full Disk Encryption:** FileVault on macOS and BitLocker on Windows must be enabled and enforced. Store the key in your MDM so it's accessible if you need to access the encrypted drive.
- **Strong Password Policy:** Require a complex password to unlock the device.
- **Screen Lock:** Automatically lock the screen after 15 minutes of inactivity.
- **System Firewall:** Ensure the built-in OS firewall is enabled (typically already set as default).
- **Automated Patch Management:** Use your MDM to enforce OS updates. A reasonable policy is to "nudge" users with notifications for 7 days, then force the update and reboot.

Spec Recommendations (2025)

Role	Model	Minimum Specs	Our Rationale
Standard Employee	MacBook Air 14" or or Lenovo T14	16GB RAM 256GB SSD	High-quality, reliable business-grade machines for 90% of roles (sales, marketing, ops, etc.).
Engineer / Designer	MacBook Pro 14" or Lenovo P16	32GB RAM 1TB SSD	These roles are your most expensive hires; their time is a valuable asset. Don't slow them down with an underpowered machine.
Executive / Corp	MacBook Air 14" or Lenovo Carbon X1	16-32GB RAM 512GB SSD	Lightweight but still powerful, offering flexibility for travel without sacrificing performance.

For Your Auditor: Key Artifacts

Your MDM is a goldmine of evidence for compliance. Be ready to generate these reports on demand:

- A complete inventory of all corporate devices, tied to the assigned user.
- Fleet-wide compliance reports for key controls like disk encryption and OS patch levels.
- A log of devices that have been remotely locked or wiped during offboarding.



SECURITY

TL;DR Unaddressed security gaps create compounding risks that grow faster than any other technical challenge. Prioritize high-impact wins that cut real-world threats in weeks, not months. Focus on MFA, EDR, immutable backups, and secure remote access.

Pragmatic Security to Protect the Lifeblood of Your Company

At Series A, a ransomware attack or exposure of your IP and company data can literally *kill your company*. The goal isn't perfect security—it's to pragmatically neutralize the most likely threats. We focus on the 80/20 rule: which controls will mitigate 80% of your real-world risk? For a startup, this means defending against stolen credentials and compromised laptops.

For compliance (SOC 2, ISO) pushes, working with an MSP partner (like Lerner Solutions) can eliminate the panic sprints we often see when companies try to catch up later.

The Priority Checklist

Control	Why	Impact	Effort	Notes
Enforce Phishing-Resistant MFA	Stops attackers even with a valid password. This is your single most effective control.	High	Low	Built into Google Workspace/M365. Enforce it by default on day one.
Deploy Endpoint Detection & Response (EDR)	Provides the visibility to detect and contain a compromise on an employee's laptop.	High	Medium	Deploys easily via MDM. Essential for detecting threats that bypass prevention.
Enable and Test Immutable Backups	Your only escape hatch from a ransomware attack. They are useless unless proven to be recoverable.	High	Medium	Most cloud services offer this. The key is to test your restore process annually.
Secure Remote & Contractor Access	Contractors and remote engineers are a common entry point. Lock down their access with a modern tool.	High	Medium	A ZTNA tool is an essential for any company with engineers accessing production systems.
Log All Administrative Activity	You cannot investigate an incident without an audit trail. This is also a baseline compliance requirement.	Medium	Low	This is a simple toggle in most SaaS tools. The initial setup is fast; centralizing the logs is a higher-effort task for later.

DÉJÀ VU? IT'S BY DESIGN.

You'll notice some concepts, like MFA and EDR, appear in multiple chapters. This is intentional. Modern IT security is about layers, not silos. Here's the mental model to clarify things:

- **Identity & Access** is about the USER (managing who can log in)
- **Devices & MDM** is about the ENDPOINT (managing the what they log in from)
- **Security** is the STRATEGY that leverages both (which actions provide the right protection)



Client Since 2018

NETWORKING

TL;DR A consumer-grade network won't survive scale, and neither will a poorly designed & configured enterprise-grade network. Build strong foundation on cloud-based equipment using redundant ISPs, network segmentation, and docs to support growth.

Reliable, Resilient, and Simple

Networking often feels secondary until it breaks—then it halts the entire business. By Series A, you need enterprise-grade connectivity. The goal isn't complexity; it's building a structured and reliable foundation.

- Keep the design simple: one network for corporate devices, one for guests, and separate networks for sensitive systems.
- Document everything—every cable, port, and IP scheme—so that future growth doesn't rely on tribal knowledge.

The Decision Matrix: Foundational Networking Choices

Decision Area	Base Recommendation	Upgrade Triggers
ISP Strategy	Single business fiber line with LTE/5G failover → **Why:** Cheap insurance so one fiber cut doesn't halt the business.	**If:** High density workspace, multi-site expansion, or high uptime expectations → **Then:** dual ISPs required to meet resilience expectations.
Network Stack	Properly designed & configured cloud-managed stack (Meraki, Aruba) → **Why:** Strong features with minimal overhead.	**If:** More control over network traffic or security/audit reqt's → **Then:** Move to advanced enterprise gear (Cisco, Palo Alto).
Firewall Vendor	Use your network stack's built-in firewall → Why: Avoids premature cost and admin burden.	**If:** Compliance/security review requires advanced controls → **Then:** Deploy a dedicated NGFW (e.g., Palo Alto, Cisco).
Network Segments	Introduce networks for Corp, Guest, IoT, etc. → **Why:** Covers 90% of risk without over-engineering.	**If:** You add POS systems, contractors, or regulated workloads → **Then:** Introduce dedicated networks for isolation.
Remote Access	Modern VPN → **Why:** Enough for small contractor use and remote staff.	**If:** You grow contractor-heavy or provide production system access → **Then:** Implement ZTNA with posture checks.

DATA & SAAS GOVERNANCE

TL;DR As headcount and apps grow, data quickly sprawls across dozens of systems. To prevent risk and waste, you must maintain complete SaaS inventory, assign ownership for access, set safe sharing defaults, and log all critical activity from day one.

Taming the SaaS Sprawl

By Series A, most companies have already adopted 30-50 SaaS tools without a central plan. Marketing, sales, product, and finance all bring in their own apps, creating a "digital landfill." Without governance, this sprawl creates three critical business risks:

- **Security Risk:** Orphaned accounts from former employees are left with active access to sensitive company data.
- **Compliance Risk:** There is no audit trail for where sensitive customer data lives or who can access it, making it impossible to pass security reviews.
- **Financial Waste:** Unused licenses, redundant subscriptions, and a lack of negotiating power drain your budget.

The solution isn't to block teams from adopting tools. It's to add a lightweight structure that turns governance into a growth enabler instead of a blocker.



Governance Gut Check

Visibility
Can you produce a complete list of all your SaaS applications and their total annual cost in under 10 minutes?

Ownership
If an employee requests access to a sensitive financial tool, is there a clear, documented owner who is responsible for approving it?

Access
If you offboarded a senior employee right now, are you 100% confident you could deprovision them from every single application they had access to?

Sharing
Is it possible for a well-meaning employee to accidentally share, for example, sensitive investor documents with the entire internet via a public link?

Quick Wins to Get Started

- **Set Sharing Defaults:** In your Google Workspace or M365 admin console, set the default for link sharing to "Private." Disable the ability for non-admins to make files public.
- **Enable Audit Logging:** Go into your top 5 most critical applications (e.g., Google/M365, Slack, Salesforce, GitHub, AWS) and ensure audit logging is turned on.
- **Create Your v1 SaaS Inventory:** Integrate your finance/spend management tool with your IdP to export your first real list of SaaS subscriptions.

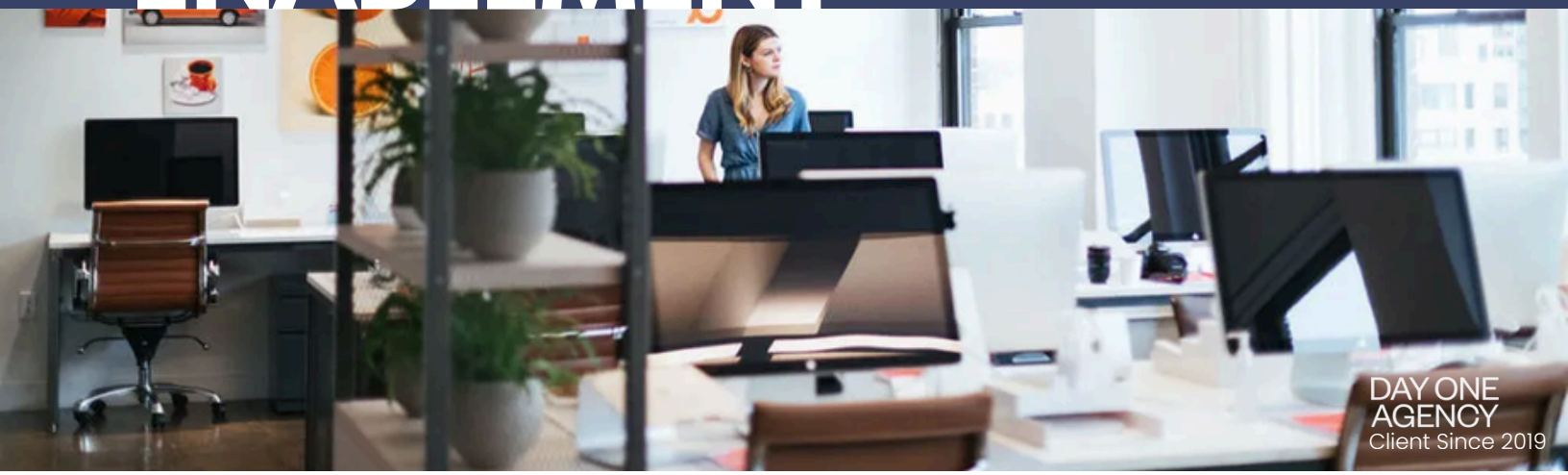
Avoiding Common Pain Points

Control Area	Common Pain Point	Best Practice	Owner
SaaS Inventory	Teams add apps ad hoc; no single list; finance doesn't know true spend.	Maintain a single tracker tied to IdP + finance; upgrade to SMP once more than 50 apps.	Primary: IT Secondary: Ops
Access Reviews	IT runs quarterly reviews manually; delays and missed removals common.	Automate reviews and assign accountability to business owners.	Joint: IT + Dept. Leads
Data Sharing	Employees accidentally share directories instead of doc, or share file with improper controls ("everyone with link")	Default all sharing to private in Google/M365; layer in DLP alerts for sensitive data.	Primary: IT Secondary: Security
Data Retention	Deleted files linger indefinitely; ex-employees' data accumulates.	Enforce auto-delete policies; evolve to classification-based retention as you grow.	Primary: Legal Secondary: IT
Audit Logging	Logs exist but are spread across tools; no single source for investigation.	Enable logging in core apps (Google, Slack, GitHub); centralize later with SIEM.	Joint: IT + Security
Data Ownership	Nobody knows who "owns" access; requests pile up in IT.	Assign each system to a dept. lead; require periodic review.	Primary: Dept. Leads Secondary: IT



Functional Deep Dives
Identity & Access
Devices & MDM
Security
Networking
Data & SaaS Governance
Workforce Enablement
Policies, Procedures & Docs

WORKFORCE ENABLEMENT



TL;DR Ad-hoc support doesn't scale. Transition from a reactive Slack channel to a ticketing system with SLAs with clear quality standards to deliver strong employee experience. Master the employee lifecycle (Joiner, Mover, Leaver) to ensure consistency & security.

From Reactive Firefighting to Proactive Enablement

At Series A, your support function must evolve from a reactive "help desk" to a proactive "workforce enablement" engine. Getting this right is a massive driver of employee productivity, security, and morale. The two most critical components of this evolution are:

- Begin introducing automation to the employee lifecycle (Joiner, Mover, Leaver)
- Improve your day-to-day support (e.g., help desk support)

Structuring Day-to-Day Support

As you scale past 50 employees, a shared #ask-IT Slack channel becomes a black hole of missed requests and untracked work. You must transition to a formal ticketing system (like Zendesk, or HaloPSA when working with an MSP like Lerner Solutions). This is not about creating bureaucracy; it's about ensuring every request is tracked, prioritized, and resolved in a timely manner.

Start by defining simple Service Level Agreements (SLAs) to set clear expectations:

- **Critical (e.g., "I can't work"):** 30-min or less response, 4-hour resolution
- **Standard (e.g., "I need access to a new tool"):** 4-hour response, 24-hour resolution
- **Low (e.g., "Question about a feature"):** 24-hour response, best-effort resolution

69%
of employees likely to stay for 3 years after a great onboarding experience.

10.5 days
workdays lost per employee, per year due to minor tech disruptions and delays.

63%
of organizations may have ex-employees who can still access corporate data and systems.

If your internal IT team is spending more time firefighting than improving systems, or if onboarding & offboarding mistakes start slipping through the cracks, partnering with an MSP helps rebalance the load.

Signs of Strain & How to Fix Them

Capability	Signs You're Underbuilt	Recommendation
Staffing Model	Ticket backlog >5 days, execs escalate issues, and no one clearly owns IT.	Add dedicated Head of IT and use an MSP like Lerner to create accountability and stabilize service levels.
Requests	Requests come through Slack or email and often get lost, with no central queue or reporting.	Implement ticketing system (e.g., Zendesk or platform integration with Slack); Lean on MSP for coverage during peaks or off-hours.
Employee Lifecycle	Offboarding takes hours, access removals are missed, and new hires often wait for laptops.	Tie HRIS to IdP and MDM to automate basic on/offboarding workflows, reducing risk & improving experience.
Knowledge	Employees repeatedly ask the same "how do I…?" questions and answers live in DMs.	Publish top FAQs in a shared system (e.g., Hudu, Notion) to improve consistency and deflect tickets.
Shadow IT	Use of unapproved SaaS apps, receipt of unexpected invoices	Streamlined approval & tracking process that balances need for security & financial oversight with team's need for speed and the right tools
Metrics	No data on ticket volume or response times, leaving no basis for planning.	Track ticket volume and response times to establish a baseline for capacity planning and service performance.
Automation	IT spends time manually resetting passwords and provisioning common apps.	Automate the top 3–5 repetitive tasks (e.g., password resets, app adds) or scripts to free IT time; partner with MSP for specialized workflows.
Hardware Lifecycle	Spreadsheets for laptops and devices are outdated, with little visibility into who has what.	Use inventory system; maintain a 5–10% spare pool; use MSP for staging, shipping, & receiving devices.
Employee Experience	IT is only noticed when things break, and employees express frustration.	Position IT as a proactive partner by surveying satisfaction and fixing the top friction points.

POLICIES PROCEDURES & DOCS

TL;DR These materials are not a project; they're a daily discipline that turns tribal knowledge into a durable company asset. Start with a few critical, plain-language policies in a centralized knowledge base, and ensure your Incident Response plan is tested.

Your IT Operating System

Policies, procedures, and documentation aren't busywork — they're the scaffolding that holds IT together. When they're missing, critical knowledge gets trapped in Slack or Teams threads or inside one person's head. The result is predictable: onboarding drags, offboarding is incomplete, and the employee experience depends on who happens to answer a ticket that day.

The Series A Trap

The bigger danger is waiting until an auditor, enterprise customer, or incident forces documentation. That scramble produces rushed policies, messy artifacts, and rework — leaving you with blinders that don't reflect reality and little evidence you're actually following them.

Evidence for Auditors

Policies alone aren't enough. Auditors will ask for proof that they're followed in practice. Capture these proactively:

- Runbook repositories with timestamps or version history.
- Signed or HRIS-tracked policy acknowledgments.
- Screenshots or reports from IdP, MDM, or ticketing systems.

What We See Go Wrong

Lack of Upkeep
Policies written once to pass an audit, then never touched again. They drift out of sync with reality, leaving you unprepared for incidents and the next audit.

Chaotic File Structure
Docs scattered across Google Drive, Notion, Asana, and Slack. No one knows where the latest version lives, so employees waste time or use outdated instructions.

Usability Issues
Policies and KB articles written in dense legalese or long prose. Nobody reads them, which means they don't change behavior or reduce risk.

Ownership is Undefined
Runbooks and policies created without a clear owner. With no one accountable for upkeep, they quickly become outdated and dangerously unreliable.

Failure to Adopt Culture
Defeat "tribal knowledge" by creating a single, up-to-date knowledge base that everyone contributes to, making critical information an institutional force that anyone can rely on.

36%
reduction in support ticket volume can be achieved by implementing a self-service knowledge base

70%
of digital transformation projects fail due to lack of documented processes

50%
of all network downtime is caused by unplanned changes made without following a documented procedure

Documentation & Policy Roadmap

Category	Recommendation	Description	Priority
Operational IT Docs	**Incident Runbooks**	Step-by-step instructions for top IT incidents (password resets, VPN, email outages). Include commands, screenshots, and escalation paths.	High
	System Configurations	Document baseline settings for IdP, MDM, EDR, firewalls, and backups. Store in version-controlled repo.	High
	Joiner/Mover/Leaver Checklists	Checklists for onboarding, role changes, and offboarding. Cover accounts, devices, access removal, and notifications.	High
Employee Knowledge	**Knowledge Base**	Central repository (Notion, Confluence, Hudu) with FAQs like Wi-Fi, Zoom, app logins, and printing. Indexed and searchable.	Med
Core Policies	**Incident Response Plan**	Playbook for detecting, containing, and remediating security incidents. Define roles (IT, Legal, Comms); be sure to test annually.	High
	Acceptable Use Policy	Defines how employees may use company systems, devices, and data. Covers security, privacy, and restrictions (e.g., no personal Dropbox).	Med
	Information Security Policy	High-level statement of security commitments. Outlines governance, responsibilities, and baseline requirements. Parent doc for all other policies.	Med
Extended Policies	**Change Management Policy**	Process for planning, testing, approving, and documenting system changes; includes risk tiers and rollback steps.	Med
	Vendor Risk Management Policy	Framework for evaluating third-party vendors. Require SOC 2/ISO reports or questionnaires. Review annually.	Med
	Additional Policies	Data Retention, Remote Work, Encryption Standards, etc. on case-by-case basis.	Case by Case

03
QUICK REFERENCES

One-Page Cheat Sheet
Compliance Checklist
Budget Benchmarks
Staffing Models
Recommended IT Stack
IT Health Check
Jobs to Be Done



Client Since 2024

ONE-PAGE CHEAT SHEET

Capability	Base Recommendation	Upgrade Triggers
Identity & Access	Use IdP (Okta) as control plane with MFA everywhere; extend SSO to critical apps; adopt PAM (Keeper) when needed; capture audit evidence (access reviews, deprovisioning).	**If:** Headcount >200, multi-office, or enterprise deals → **Then:** Expand SSO coverage, enforce conditional access, and automate access reviews.
Device Management	Deploy zero/near zero-touch provisioning with MDM; enforce encryption, patching, and lock/wipe; maintain a 5-10% spare pool	**If:** Devices >200, formal audit, contractor-heavy → **Then:** Proactive hardware refresh (3 years), compliance reporting
Security	Enforce MFA, deploy EDR on all devices, maintain immutable backups, enable basic email security (SPF/DKIM/DMARC), and provide secure remote access (ZTNA or VPN).	**If:** SOC 2 required, enterprise deals, or incident occurs → **Then:** Add SIEM, vulnerability scans, and a formal incident response program.
Networking	ISP with LTE/5G failover; cloud-managed firewall + network stack; simple 3 network segmentation; secure remote access via VPN or simple ZTNA.	**If:** Multi-site, high-density workspace, or uptime challenges → **Then:** Add redundant ISPs, enterprise NGFW, and expanded segmentation.
Data & SaaS Governance	Track SaaS via IdP (Okta); run access reviews; default sharing to private; enforce retention policies; enable audit logging; assign ownership.	**If:** SaaS apps >50 or license waste >15% → **Then:** Deploy SaaS mgmt platform and formalize governance reviews.
Workforce Enablement	Hire MSP or implement basic ticketing system; publish a knowledge base; script top 3-5 repetitive tasks; create lightweight runbooks.	**If:** Tickets exceed SLA or headcount >200 **Then:** Formalize SLAs, expand automation, and add reporting/escalation.
Policies & Documentation	Prioritize incident runbooks, system configs, on/offboarding checklists, and incident response plan; capture evidence artifacts.	**If:** Pursuing SOC 2, ISO 27001, or enterprise contracts → **Then:** Expand policy set and integrate with compliance automation.
Compliance	Prep for SOC 2 or SOX with documented policies, evidence collection, and annual risk assessment; manage artifacts manually at first.	**If:** Enterprise/regulated deals require proof → **Then:** Use compliance automation (Vanta/Drata) and centralize evidence collection.
Budgeting	Track IT spend; allocate SaaS by department; expect 15–20% waste buffer from SaaS sprawl and shadow IT.	**If:** Annual IT spend >$1M or waste exceeds buffer → **Then:** Formalize forecasting, vendor negotiations, and procurement review.
Employee Experience	Use checklists for onboarding; survey annually; position IT as partner by reducing friction and publishing IT roadmap.	**If:** Headcount >200 or employee churn rises → **Then:** Automate onboarding, survey quarterly, and add self-service IT resources.
IT/Business Alignment	IT lead participates in exec meetings; ensure IT is represented in strategic discussions.	**If:** Headcount >200 or recurring IT issues affect business → **Then:** Establish CIO/CISO role, strategic roadmap, and board reporting.

Quick References
One-Page Cheat Sheet
Compliance Checklist
Budget Benchmarks
Staffing Models
Recommended IT Stack
IT Health Check
Jobs to Be Done

COMPLIANCE CHECKLIST

This checklist maps common SOC 2 and ISO 27001 requirements to the specific "evidence" you'll need to provide an auditor. Use it to get organized and ensure you are ready before your first audit.
A compliance expert like Lerner Solutions can significantly improve audit readiness.

Domain	Control Requirement	Artifact to Maintain	Internal Owner
Identity & Access	Enforce MFA, least privilege, offboarding.	Access control policy, quarterly access review, IdP logs.	IT / Security Lead
Devices & MDM	All laptops enrolled in MDM, encryption on, patching enforced.	MDM compliance reports, encryption proof, baseline config, patch history.	IT
Security Monitoring	Log collection and monitoring of critical systems.	SIEM or log exports, alert workflow, incident tickets.	IT
Change Management	Document and review changes to production systems.	Change management policy, approval records, Git commit logs.	Eng / IT
Vendor Management	Review vendors before use, track risk ratings.	Vendor risk policy, vendor list, SOC 2 reports, signed DPAs.	Security / Legal
Incident Response	Documented IR plan, test at least annually.	IR policy, tabletop exercise report, incident tickets.	Security / IT
Backups & Recovery	Regular, tested backups with immutability.	Backup logs, recovery test evidence, RPO/RTO defined for critical apps.	IT / Ops
Business Continuity	Define continuity plan, test periodically.	BCP document, test evidence, comms plan.	Exec / Ops
Training & Awareness	Annual security training for all employees.	Training logs, completion reports, Phish test results.	People Ops / IT
Risk Assessment	Conduct risk assessment at least annually.	Risk register, assessment report, mitigation plan.	Security / Exec Sponsor
Physical Security	Secure office access controls (badges, locks).	Visitor logs, badge system reports, physical security policy.	Ops
Data Governance	Define data retention, classification, and ownership.	Data retention policy, SaaS inventory, data map.	IT / Legal
Policies	Formal, approved policies reviewed annually.	AUP, InfoSec Policy, Change Mgmt Policy, Vendor Policy, IR Plan.	Leadership / IT

Quick References
One-Page Cheat Sheet
Compliance Checklist
Budget Benchmarks
Staffing Models
Recommended IT Stack
IT Health Check
Jobs to Be Done

BUDGET BENCHMARKS

3 Key Cost Drivers

- **SaaS Licenses:** Fastest-growing line item. Every new hire will often require seats for 5–10 platforms, and without governance unused licenses quietly drain budget. DLP, security suites, and compliance software can double costs in regulated industries.
- **Hardware & Infrastructure:** Laptops, monitors, and spares are recurring and lumpy. Expect refresh cycles every ~3 years, plus spikes from growth hiring. Failure to budget for spares leads to costly rush orders and downtime. A crucial line item is the physical buildout of a new office, which can cost $50k-$250k+ depending on type.
- **People/Partners:** Internal IT staff or MSP contracts scale with headcount and compliance. Assume one helpdesk staff member for every 75-150 employees. Adding adding 24/7 emergency coverage or audit prep can quickly grow spend.

Where Money Disappears

- **SaaS Sprawl:** Redundant tools, orphaned licenses, no volume leverage.
- **Neglected Licenses:** Seats keep running after employees leave.
- **Overprovisioning:** Paying for storage/seats you don't actually use.
- **Enterprise Too Soon:** Buying advanced platforms before the org is ready.
- **Contract Lock-Ins:** Multi-year deals outgrown before they expire.
- **Hidden Integrations:** Connectors (Zapier, iPaaS) multiply quietly.
- **Soft Costs:** Training, integrations, and admin often 1.5–3x license price.

Industry Benchmarks

Software

- 3–5% of revenue
- Heavy SaaS spend, compliance, and security tooling. High on software; low on physical hardware. Higher if you're in a regulated industry (FinTech, HealthTech) or sell to enterprise customers.

Professional & Finance Services

- 4–6% of revenue
- Strict compliance (FINRA, HIPAA), client data security, and data protection tools. Highest spend if regulatory burden and/or directly handling financial transactions.

E-Commerce & DTC

- 2–4% of revenue
- Endpoint devices, warehouse tech, and logistics support. High on physical assets; lower on complex software licenses. Higher if you operate physical retail locations or have a complex supply chain.

Retail & Restaurants

- 2–3% of revenue
- Multi-site networking, Point-of-Sale (POS) hardware, and field support. Lowest percentage of revenue, but high spend on distributed hardware. Higher if you have a franchise model or complex POS integrations.

Quick References
One-Page Cheat Sheet
Compliance Checklist
Budget Benchmarks
Staffing Models
Recommended IT Stack
IT Health Check
Jobs to Be Done

STAFFING MODELS

Below are some common examples & thoughts on how to choose the right IT staffing model based on business model, size, risk, compliance, and complexity.

Scenario	Base Recommendation	Model Shift Trigger
SaaS	Hybrid model is likely best. Internally, focus on IT strategy and application ownership. Hire MSP for user support, device management, security, and SaaS administration.	**If:** Headcount >200 → **Then:** Internally, formalize IT budgeting and vendor mgmt. Expand MSP scope to advanced endpoint security for all critical apps.
		If: Globally team or offshore developers → **Then:** Internally, establish regional IT points of contact. Expand MSP scope to 24/7 help desk coverage and secure int'l device logistics.
		If: Onboarding >20 hires per quarter. → **Then**: Internally, build IT knowledge base and streamline departmental workflows. Expand MSP scope to automated user provisioning and day-one support.
D2C / E-commerce	Hybrid model is likely best. Internally, manage core e-commerce and fulfillment tech stack. Hire MSP for corporate IT support and infrastructure management.	**If:** Fulfillment stack complexity or seasonal demand creates performance risk → **Then:** Internally, build a dedicated ops/engineering team to manage core stack. Expand MSP scope to infrastructure scaling, 24/7 monitoring, and co-managed platform support.
Multi-Site Retail or Restaurants	Hybrid model is likely best. Internally, focus on retail systems (POS, inventory). Hire MSP like Lerner Solutions with national field tech coverage for store openings and on-site support.	**If:** >5 new locations per quarter → **Then:** Internally, create dedicated new store opening program lead. Expand MSP scope to create and manage hardware & software deployment playbook and centralize all frontline support.
High-Compliance Need (FinTech, HealthTech)	Hybrid model is non-negotiable. Internally, hire compliance lead (e.g., a CISO) to focus on risk and compliance strategy. Hire MSP for implementing and managing audit-ready technical controls.	**If:** Formal audit (SOC 2, HIPAA), new regulatory markets, enterprise deals → **Then:** Internally, dedicate a resource to GRC. Expand MSP scope to co-managed SIEM, continuous vulnerability scanning, and formal evidence collection.
Professional Services	Fully outsourced model is likely best. Internally, focus 100% on clients & core business. Hire MSP to manage all IT functions, from strategy and support to security.	**If:** Clients require security reviews or data handling assurances → **Then:** Internally, assign partner to oversee client-facing security and compliance. Expand MSP scope to security questionnaires and auditable logs for client data access.
Heavy Use of Contractors & Third Parties	Hybrid model is likely best. Internally, focus on defining access policies and data ownership. Hire MSP for high-volume, rapid onboarding and offboarding.	**If:** Contractor roles require access to sensitive internal systems or client data → **Then:** Internally, implement formal third-party risk management process. Expand MSP scope to identity and access management automation with role-based access controls and auditable logs.
Hypergrowth (Hiring 50+ in a Quarter)	Hybrid model is likely best. Internally, focus on the long-term technology roadmap. Hire MSP to support internal roadmap vision, absorb the surge in onboarding, and support ticket volume.	**If:** Hiring splits between technical (e.g., developers) and non-technical roles, or across multiple office hubs → **Then:** Internally, create distinct IT onboarding tracks for different roles. Expand MSP scope to specialized software deployments (for devs) and provide on-site support at new office hubs.
Hardware-Heavy (Lab, R&D, Manuf.)	In-house led hybrid model is likely best. Internally, focus on managing specialized lab or R&D equipment. Hire an MSP for standard corporate IT (networking, cloud systems, user support).	**If:** Multiple facilities, multiple geographies → **Then:** Internally, focus on standardizing IT processes across sites. Expand MSP scope to on-site support for new locations and managing network buildouts.

Quick References
One-Page Cheat Sheet
Compliance Checklist
Budget Benchmarks
Staffing Models
Recommended IT Stack
IT Health Check
Jobs to Be Done

RECOMMENDED IT STACK

This cheat sheet maps the core IT domains to recommended tools and upgrade triggers, so you know what to use now and when to level up.

Domain	Base Recommendation	Upgrade Triggers
Identity & Access	Okta for SSO/MFA; Keeper for privileged access management (PAM)	**If:** >200 employees or advanced security needs → **Then:** Upgrade to Okta Adaptive MFA and integrate with HRIS (Workday, BambooHR).
Password Management	Keeper for password management (1Password as alternatives for basic vaulting)	**If:** Engineering scale increases or secrets sprawl → **Then:** Add HashiCorp Vault for dev/infra secrets and enforce vault-based workflows.
Devices & Endpoint	Jamf for macOS MDM; Intune for Windows MDM; Platform-native for encryption (FileVault for macOS ; BitLocker for Windows)	**If:** Device count >200 or SOC 2 audit required → **Then:** Layer compliance dashboards in Jamf/Intune or add Kandji for Apple compliance mgmt.
Endpoint Security	Platform-native (Microsoft Defender) or third-party (Sophos) for EDR/XDR	**If:** Pursuing SOC 2 or enterprise contracts → **Then:** Add CrowdStrike Falcon for EDR and Cloudflare Access for ZTNA.
Email & Threat Protection	SPF/DKIM/DMARC for all domains; KnowBe4 for awareness training; Check Point Harmony Email or Barracuda for threat protection	**If:** Sensitive data (e.g., PHI/PII) at scale or compliance requires layered security → **Then:** Full-suite secure email gateway (Mimecast or Proofpoint) for integrated DLP, encryption, and archiving.
Networking	Meraki for cloud-managed network stack; Aruba as alternative	**If:** Compliance-heavy environment → **Then:** Move to Cisco Catalyst for enterprise switching or Palo Alto NGFW for advanced security.
ZTNA & Remote Access	Cloudflare Access for zero-trust remote access	**If:** Contractor-heavy, global offices, or legacy VPN deprecation → **Then:** Expand to full ZTNA suite (Zscaler, Palo Alto Prisma Access).
Data & SaaS Governance	Google Workspace or M365 for sharing defaults; Okta, Torii, Tropic for SaaS mgmt	**If:** >100 SaaS apps, license waste >15%, or DLP/regulatory needs arise → **Then:** Expand automation of chosen platform or adopt Microsoft Purview/Netskope for DLP/classification.
IT Support & Lifecycle	Zendesk, Halo PSA, or Freshworks for ticketing & asset tracking; Okta Workflows for lifecycle management	**If:** Ticket volume >200/month, SLA breaches, or audit pressure → **Then:** Hire MSP like Lerner Solutions, or dedicated ITSM platform (Freshservice) and IGA tool (Opal, ConductorOne).
Backup & Recovery	Acronis for SaaS/endpoint backup; Spanning for SaaS backup	**If:** Customers require DR testing or strict RPO/RTO → **Then:** Add Druva for SaaS/endpoint backup or Rubrik for enterprise DR.
Policies & Documentation	Use ticketing system for knowledge base and documentation; Hudu as alternative for docs	**If:** Pursuing SOC 2/ISO 27001 → **Then:** Integrate with Vanta or Drata for compliance automation and evidence mgmt.
Compliance	Vanta for SOC 2 readiness; Drata as alternative	**If:** Enterprise/regulated customers → **Then:** Use Drata for ISO 27001 and pair with Splunk, SentinelOne, Splunk for SIEM/continuous monitoring.
Vendor Risk Management	Notion or Google Drive for vendor evidence collection; Standardized questionnaire (e.g., SIG Lite) for manual risk assessment.	**If:** Pursuing SOC 2/ISO 27001, or if enterprise customers require vendor due diligence → **Then:** Vendor Risk Management platform (Vanta, Drata) to automate security questionnaires and evidence collection.
Logging & Auditing	Native audit logs in Google Workspace, M365, Slack, Salesforce, GitHub, and AWS	**If:** Centralized log correlation or SOC 2 continuous monitoring needed → **Then:** Implement SIEM platform (SentinelOne, Datadog, Splunk) for aggregation, alerting, and evidence retention.

Quick References
One-Page Cheat Sheet
Compliance Checklist
Budget Benchmarks
Staffing Models
Recommended IT Stack
IT Health Check
Jobs to Be Done

IT HEALTH CHECK

Answer each question with a simple "Yes" or "No." This isn't a deep audit, but an honest gut check to identify your biggest risks and opportunities.

Domain	Key Questions	Total Points (Yes = 1 / No = 0)
01 **Identity & Access**	• Are all core apps behind SSO? • Is MFA enforced for every account? • Are admin & privileged access accounts reviewed quarterly? • Is offboarding automated through your identity platform?	
02 **Devices & MDM**	• Are 95%+ of devices enrolled in MDM? • Are OS and browser updates auto-applied? • Do you maintain a clean spares inventory? • Can you remotely wipe any lost/stolen device?	
03 **Security**	• Is EDR live and reporting on all endpoints? • Do you run quarterly vulnerability scans? • Can you restore from immutable backups within 24h? • Is email security (SPF/DKIM/DMARC) configured? • Is there ongoing security awareness training for employees?	
04 **Networking**	• Is guest Wi-Fi segmented from corporate? • Is ISP failover or backup connectivity in place? • Are firewall/VLAN rules reviewed at least annually?	
05 **Data & SaaS Governance**	• Is there a current SaaS inventory? • Are unused licenses deprovisioned monthly? • Are data retention rules configured in major apps? • Is sensitive data protected with DLP or equivalent?	
06 **Workforce Enablement**	• Are SLAs tracked for tickets? • Does onboarding include automated account/device setup? • Does offboarding remove all access in <1h? • Is there a searchable knowledge base for employees?	
07 **Policies, Procedures & Docs**	• Do you have an Acceptable Use Policy in place? • Has the IR plan been tested in the past 12 months? • Are all policies centralized and accessible? • Is documentation updated after each major change?	
	Total Score:	



23 to 28 Points 🟢 **Healthy**
17 to 23 Points 🟡 **Needs Improvement**
0 to 17 Points 🔴 **At Risk**

JOBS TO BE DONE

Open the First Office

- Lock in your primary fiber and 5G backup ISP 60 days out (lead times are real).
- Develop structured cabling plan with thoughtful design partner like Lerner Solutions
- Document your network with rack diagrams and port maps before it goes live.
- Deploy a single-vendor, cloud-managed stack (e.g., Meraki) for simple remote management.
- Secure corporate Wi-Fi with enterprise authentication tied to your IdP (no shared passwords).
- Install and test physical security controls from day one (access control, cameras).

Hire 50 People in 90 Days

- Lock in zero-touch deployment workflow (Jamf for macOS and Intune for Windows)
- Build a spare hardware pool (5% of fleet size) to prevent new hire delays.
- Automate the Joiner, Mover, Leaver (JML) process, triggered by your HRIS
- Audit SaaS licenses weekly during the hiring blitz (costs spiral fast).
- Proactively expand Help Desk and IT support capacity to handle the increased load.
- Pre-load a "First Day" KB article to cut duplicate tickets.

Pass the First SOC 2

- Engage a reputable third-party firm for a readiness assessment before the real audit.
- Enforce your core technical controls (MFA, MDM, EDR) across 100% of the fleet.
- Establish your core policy library (InfoSec, AUP, IR are non-negotiable).
- Start capturing evidence now (screenshots, logs, tickets); don't wait for the audit to begin.
- Conduct and document quarterly access reviews for all critical systems.

Add International Contractors Safely

- Deploy a ZTNA solution for granular, application-level access (traditional VPNs are too broad).
- Issue named accounts for all contractors; strictly prohibit any shared logins.
- Leverage DLP in your core SaaS apps to monitor and block unauthorized data exfiltration.
- Consult legal on regional compliance rules (e.g., GDPR) that apply to contractor data.
- Define minimum security standards for contractor devices and require attestation.

Go from 1 to 10 Sites

- Partner with national MSP like Lerner Solutions to provide local "hands and eyes" support for all remote site buildouts and troubleshooting.
- Develop a standardized "office-in-a-box" template that includes your hardware bill of materials, cabling spec, and network configuration.
- Use templated configurations from your cloud-managed network vendor to ensure consistency.
- Deploy remote monitoring tools to centrally manage the health and uptime of all locations.
- Create a standardized budget template for new site buildouts to ensure predictable costs.
- Maintain an "ISP cut sheet" for each site (account #, support #, demarc photo).
- Standardize SSID naming, VLAN mapping, and IP plan across all sites.

LERNER SOLUTIONS

LET'S TALK

At Lerner Solutions, we're more than just an IT provider—we're a long-term partner in scaling your business.

Headquartered in New York, we've spent the past decade supporting some of the fastest-growing companies in the country with reliable, enterprise-grade IT infrastructure.

Contact our Founder & President, David Lerner, at david@lernersolutions.com

