SOLUTION BUILDERS®

A SOLUTION BUILDERS PLAYBOOK
2026 EDITION

A PLAYBOOK FOR INTERNAL IT LEADERS

# The Co-Managed IT Playbook.

Three staffing models decoded, an ownership matrix that ends the finger pointing, a 30 day cure for key person risk and a plan to give your team its week back.

INSIDE THE PLAYBOOK


01 Three models, decoded

02 Splitting ownership

03 Key person risk

04 Strategic capacity



**Published by Solution Builders**
Bloomington, Minnesota · www.solutionbuilders.com


**30+** YEARS

**Top 1%** OF MSPS

**98%** CSAT

WHAT'S INSIDE

# Built for the IT leader who is out of hours, not out of ideas.

You have IT talent. What you do not have is enough hours, every specialty and 24/7 coverage. Co-Managed IT fixes the math without taking away the keys. This playbook shows how internal teams add a 50+ engineer bench, enterprise tooling and round the clock coverage while keeping every decision that matters.


**01** **Co-managed vs. fully outsourced, decoded.**
Three ways to run IT, compared on coverage, cost, control and specialties. Why the middle option exists, and who it is built for.
PAGE 03

**02** **How to split ownership cleanly.**
An ownership matrix across help desk tiers, patching, security operations, projects, vendors and strategy. One owner per row, in writing, before day one.
PAGE 06

**03** **Eliminating key person risk.**
What happens when the one person who knows everything is on a beach, in a hospital or at a competitor. Vaults, runbooks, cross coverage and a 30 day cure.
PAGE 09

**04** **Freeing your team for strategic work.**
What your team does with 15 reclaimed hours a week. The time split before and after, the projects that finally ship and how to prove it to the CFO.
PAGE 12


**WHO IT IS FOR**
IT directors, IT managers and the executives they report to at companies with 25 to 500 people and a one to five person IT team.

**HOW TO USE IT**
Chapter 02 is the working session. Print the ownership matrix, fill it in with your team and bring it to the next budget conversation.

**READING TIME**
About 25 minutes cover to cover. The key person risk audit in chapter 03 takes an hour to run and is worth every minute.

SOLUTION BUILDERS®

01

# Co-managed vs. fully outsourced, decoded.

Most IT leaders hear "managed services" and picture being replaced. That is one model, and it is not this one. Co-Managed IT adds a bench, a toolset and a night shift to the team you already have. This chapter puts all three models side by side so the differences are plain.

**3**
ways to run IT: in house only, co managed, or fully outsourced

**168**
hours in a week. One in house engineer covers about 40 of them.

**4.8M**
global shortfall of cybersecurity professionals, the hardest roles to hire

**50+**
engineers on the Solution Builders bench, on call for your internal team

# Three ways to staff IT, side by side.

In house only, co managed and fully outsourced are not three price points for the same thing. They are three different answers to who owns decisions, who answers the phone at night and who covers the gaps. Here is how they compare where it matters.

| | IN HOUSE ONLY | CO MANAGED | FULLY OUTSOURCED |
|---|---|---|---|
| **Coverage** | **Business hours, best effort after** | **24/7, with a staffed SOC behind your team** | **24/7, by contract** |
| **Specialties** | **Whatever your people happen to know** | **50+ engineers across security, cloud, network and compliance** | **The provider's bench, on the provider's schedule** |
| **Tooling** | Whatever the budget allowed | Enterprise monitoring, ticketing, XDR and documentation, shared | The provider's stack, in the provider's console |
| **Control** | **Total, and so is the risk** | **Yours. You set priorities and own the decisions** | **Shared. Priorities follow the contract** |
| **Cost model** | Salaries, benefits, training, turnover | Your payroll plus a fixed monthly fee | Fixed monthly fee, per user or per device |
| **Best for** | Large teams with every specialty on staff | Companies with one to five IT staff who need hours and depth | Companies with no internal IT at all |

## Three signs you are a co managed company

- **Your IT lead is also the help desk.** The person who should be planning the ERP upgrade is resetting passwords at 4:45 p.m.
- **Nobody is watching after six.** Alerts land in an inbox and get read in the morning. Attackers know this and plan around it.
- **Every project waits for a specialist.** The firewall migration has been "next quarter" for three quarters because nobody in house has done one.

**168**

hours a week your systems need someone watching

**40**

of those hours one in house engineer can realistically cover

### What co managed is not

It is not a slow replacement of your team. The agreement names what your people own and what ours own, in writing. Your IT leader stays in charge of priorities, vendors and the roadmap. We bring the hours, the specialties and the night shift.

# The decision comes down to hours, specialties and risk.

Headcount is the wrong starting point. Start with the hours your business needs covered, the specialties it needs on call and the risk it carries when one person is out sick. The right model picks itself from there.

## Four questions that pick the model

1

### Count the hours.

Every hour the business needs IT reachable, nights and second shift included, against the hours your team can staff.

2

### List the specialties.

Security operations, cloud, networking, compliance, Microsoft 365, backup. Mark the ones you have at a senior level.

3

### Name the single points of failure.

Who alone can restore the ERP, change the firewall or call the phone vendor? Most teams count three or four.

4

### Decide what you want to keep.

Strategy, vendors, the help desk, the relationship with the business. What you keep is the shape of the agreement.

### Hours of active coverage per week, by model




Hours per week with a trained person actively watching. 168 is every hour there is. On call rotations add reach, not attention.

> **Headcount says how many people you have. Hours and specialties say how much coverage you have.**
>
> SOLUTION BUILDERS CO-MANAGED PRACTICE

FULLY OUTSOURCED

### What you hand over

- Priorities, which now follow the contract and the provider's queue.
- Vendor relationships and the history that comes with them.
- The option to bring work back in house without starting over.

CO-MANAGED IT

### What you keep, and what you add

- You keep the decisions, the vendors, the roadmap and your people.
- You add 50+ engineers, a 24/7 SOC and enterprise tooling.
- You get a written split of ownership, reviewed every quarter.

Sources: ISC2 Cybersecurity Workforce Study 2024 (4.8 million global workforce gap); coverage hours are arithmetic: 24 hours a day for 7 days is 168, and one full time engineer staffs about 40 of them. Staffing patterns from Solution Builders client engagements.

02

# How to split ownership cleanly.

Co managed arrangements fail for one reason: two teams who each think the other one has it. The fix is boring and powerful. Write down every recurring function, give each one a single owner and a backup, and review the list every quarter. This chapter hands you the matrix.

**6**
functions to assign: help desk, patching, security operations, projects, vendors, strategy

**1**
owner per row. Shared ownership is a polite name for no ownership.

**60%**
fewer support tickets at an 85 user manufacturer within 90 days of the new operating model

**90**
days from kickoff to a fully documented, fully covered split at that same client

# One owner per function, written down before day one.

This is the working page of the playbook. The matrix below is the split most internal IT leaders choose, and every row is negotiable. What is not negotiable: one name in the owner column, and one number that says the row is healthy.

## The matrix most internal IT leaders choose

| FUNCTION | OWNER | BACKUP | MEASURED BY |
|---|---|---|---|
| **Help desk and escalations** | Tier 1 your team or ours. Tiers 2 and 3 Solution Builders | The other team, same queue | Response time, time to resolve |
| **Patching and updates** | Solution Builders, automated | Your team approves exceptions | Patch compliance within 14 days |
| **Security operations, 24/7** | Solution Builders SOC | Your IT lead, for decisions | Time to detect and contain |
| **Projects and migrations** | Shared, one named lead per project | Set per project | On time, on scope, documented |
| **Vendors and licenses** | Your IT lead | Solution Builders account team | Renewals on time, no surprise true ups |
| **Strategy and budget** | Your IT lead, with a virtual CIO | Your leadership team | Roadmap reviewed quarterly |

## How to fill it in

1. **List every recurring function.** Walk a month of tickets and calendars. Anything that happens more than once a quarter goes on the list.

2. **Assign one owner and one backup.** A team, then a name. If two names want the same row, split the row until each piece has one.

3. **Agree the handoff and the number.** How work moves between the teams, and the one metric that tells you the row is healthy.

### The "shared" trap

Shared is the word that sinks co managed agreements. Patching was "shared," so nobody patched the hypervisor. If a row must be shared, split it: your team approves, our team executes.

> **If a row in the matrix has two names on it, it has zero owners.**
>
> SOLUTION BUILDERS CO-MANAGED PRACTICE

# Where the handoffs happen, and how to keep them clean.

A ticket that bounces between two teams is slower than a ticket owned by either one. Define the escalation path, the shared tools and the review cadence up front, and two teams start behaving like one bigger team.

## The first 90 days of a co managed split

**WEEKS 1 TO 2**

### Discover and document

Inventory, access review, and the ownership matrix drafted with your team in the room.

**WEEKS 3 TO 4**

### Tooling and access

Shared ticketing, monitoring, documentation, vault. Your team gets logins too.

**WEEKS 5 TO 8**

### Hand off, row by row

Patching first, then security operations, then escalations. One function a week.

**WEEKS 9 TO 12**

### Steady state

Full coverage, first monthly scorecard, matrix adjusted by what the first 60 days taught.

## The handoff agreement

- One ticket queue, one tool, visible to both teams. No side channels and no "just text me."
- Escalation targets written down by tier, with a named person on each side for the exceptions.
- Shared documentation that both teams edit. If it only lives in one team's system, it does not exist.
- A change rule: who can change what, with how much notice, and who gets told afterwards.
- A vendor rule: who calls the ISP, the software vendor, the insurer. One voice per vendor.
- A monthly scorecard reviewed together: tickets, patch compliance, incidents, projects, hours.

> **The business should feel like one IT team that got bigger, not two teams it has to referee.**
>
> SOLUTION BUILDERS CO-MANAGED PRACTICE

## Escalation ladder

| TIER | WHO PICKS IT UP | TARGET |
|---|---|---|
| **Tier 1, users** | Your help desk or ours | 15 minute response |
| **Tier 2, systems** | The team that owns the row | 1 hour response |
| **Tier 3, engineering** | Solution Builders specialist | Engaged in 4 hours |
| **Security incident** | 24/7 SOC, at once | Isolation authority, no call needed |

Planning defaults. Set your own targets in the agreement.

### Who talks to the CEO

Your IT lead does, always. We brief them, they brief leadership. One voice to the business, two teams behind it.

Sources: Solution Builders client data (85 user manufacturer: 60% fewer support tickets and 100+ hours of monthly downtime eliminated within 90 days); ITIL 4 guidance on tiered support and service level management. Response targets are planning defaults, not a service commitment.

03

# Eliminating key person risk.

Every small IT team has one person who holds the passwords, the vendor relationships and the history of why things are the way they are. That person is a single point of failure, and most companies do not notice until the day they are gone. This chapter is the audit and the fix.

**3.9**
years: median tenure of US employees. Your IT lead will eventually leave, retire or move up.

**2x**
annual salary: the high end of what Gallup estimates it costs to replace an employee

**1,900**
hours a year one engineer actually works, against 8,760 hours your systems run

**22 min**
to contain ransomware at a 42 user firm. A 24/7 SOC does not take vacation.

# Find out how much lives in one person's head.

Run this audit with your IT lead in the room, not about them. The goal is not to replace anyone. It is to make sure the business keeps running when they take the vacation they have earned.

## Six places key person risk hides

**01 Credentials**

Admin passwords, MFA devices, the domain registrar, cloud consoles, the firewall, the backup portal. One head or one spreadsheet is a finding.

**02 Vendor relationships**

ISP, phones, renewals, hardware support. Who else has the account numbers and the name of the rep who actually answers?

**03 Undocumented systems**

The script that runs the payroll export. The server nobody may reboot. The firewall rule from 2017 everything depends on.

**04 Tribal knowledge**

Why things are configured the way they are. Which users need special handling. What broke last time, and what fixed it.

**05 Recovery steps**

Can anyone else restore a server, a mailbox or the ERP database from backup tonight? Have they ever done it end to end?

**06 Approval authority**

Who can approve a change, sign a renewal or call the insurer during an incident? If every answer is one name, write it down.

### The vacation test

Send your IT lead on two weeks of vacation with no laptop and no calls. Everything that breaks, stalls or waits for them is key person risk, now visible and ready to fix. Most teams never get to run the test on purpose.

**2 wks**

the vacation test: no laptop, no calls, and a log of what stalled

**4**

eyes on every credential, runbook and vendor account. Two people, minimum.

## Score the audit

| ITEMS AT RISK | WHERE YOU STAND |
|---|---|
| 0 to 1 | Covered. Keep the documentation current and test it twice a year. |
| 2 to 3 | Exposed in places. Fix credentials and recovery first. |
| 4 to 6 | One resignation from a crisis. Start the 30 day cure on the next page. |

# Make every critical task doable by two people.

Key person risk is not solved by hiring a second person, who then becomes the second key person. It is solved by systems: a vault, a runbook library, a documented environment and a bench that already knows your network.

## The 30 day cure

**WEEK 1**

### Vault everything

Every credential into a shared vault with MFA, roles and break glass access for two leaders.

**WEEK 2**

### Document the environment

Network diagram, asset list, vendor sheet with account numbers, the ten runbooks that matter.

**WEEK 3**

### Cross cover

A bench engineer shadows your IT lead, then runs the top five tasks supervised. Gaps get written down.

**WEEK 4**

### Test it

Your IT lead takes a day off, really off. The bench runs the queue. Whatever stalls is next month's list.

## Before and after

| RISK | BEFORE | AFTER |
|---|---|---|
| Credentials | One head, one spreadsheet | Vault, MFA, two approvers, audit log |
| Recovery | One person has ever restored anything | Runbook tested by two people quarterly |
| Vendors | Contacts live in one inbox | Vendor sheet, shared mailbox, named backup |
| Knowledge | "Ask Dave" | Documentation both teams maintain |
| Approvals | One signature for everything | Two named approvers per vendor and change |
| Coverage | Vacation means exposure | 50+ engineers who already know the network |

## The minimum documentation set

- Network diagram with every site, circuit, firewall and VLAN, dated and stored where both teams can reach it.
- Asset list: servers, cloud subscriptions, licenses, warranties and renewal dates.
- Vendor sheet: account numbers, support numbers and who is authorized to call.
- Admin access map: who has what rights, where, and who approved it.
- Top ten runbooks: restore a server, restore a mailbox, onboard, offboard, patch, fail over.
- Incident contacts and the cyber insurance policy number, on paper, off the network.

> **Dave is not the problem. Dave built everything. The fix protects Dave's vacation too.**
>
> SOLUTION BUILDERS CO-MANAGED PRACTICE

Sources: US Bureau of Labor Statistics, Employee Tenure Summary, January 2024 data (median tenure 3.9 years); Gallup, "This Fixable Problem Costs U.S. Businesses $1 Trillion," 2019 (replacement cost of one half to two times salary); working hours are arithmetic: 2,080 paid hours less time off, holidays and training. Case data from a Solution Builders client, 42 users, accounting.

04

# Freeing your team for strategic work.

Nobody hires an IT director to reset passwords. Yet that is where the week goes when the same three people own the help desk, the patching, the projects and the strategy. This chapter shows what changes when routine work has a second home, and how to make the case in numbers.

**70%**
of a typical internal IT week goes to tickets, patching and firefighting before the split

**15**
hours a week reclaimed per internal engineer in a typical co managed engagement

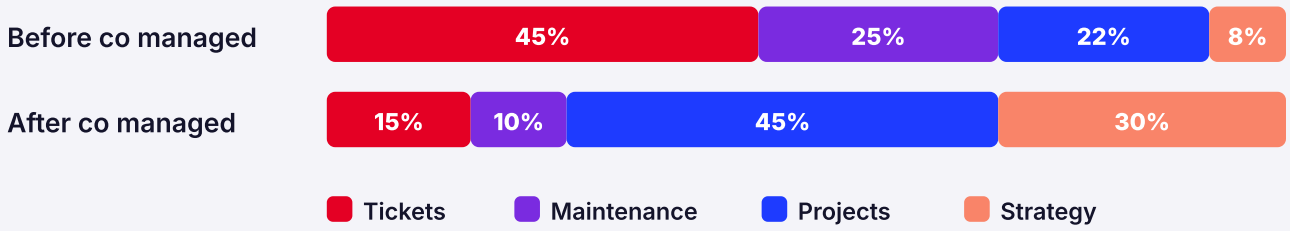
**100+**
hours of monthly downtime eliminated at an 85 user manufacturer in 90 days

**11.4%**
of project investment wasted through poor project performance, per PMI

# Where the week goes, before and after the split.

The chart below is the pattern we see across co managed engagements. The hours do not disappear. They move to the work only your team can do: the ERP upgrade, the security roadmap and the conversations with the business that never happened because the queue was full.

**Where a three person internal IT team's week goes**




Illustrative shares of weekly hours, drawn from Solution Builders client engagements. Maintenance includes patching, backups and firefighting. The team size did not change. The work did.

## What teams do with 15 hours a week back

**01** **Finish the project that keeps slipping.**
The ERP upgrade, the Teams Phone rollout, the warehouse Wi-Fi. A named owner, a real deadline and no ticket interruptions.

**02** **Own security instead of reacting to it.**
Quarterly access reviews, a risk register, a tabletop exercise. The SOC watches, your team governs.

**03** **Sit with the business.**
Shadow operations and finance for a day each quarter. Most of the best IT ideas come from there, not from a vendor.

**04** **Build the roadmap and the budget.**
A three year plan with refresh dates and a defensible number, instead of surprise purchases every quarter.

**05** **Learn something.**
Certifications, a cloud lab, a conference. Teams that have time to learn are the teams that stay.

**15**
hours a week reclaimed per internal engineer, typical engagement

**60%**
fewer tickets at an 85 user manufacturer once routine work had a second home

### The work does not disappear

Tickets still get answered, patches still get applied, alerts still get triaged. They get done by a team built to do them at scale, with tooling and shift coverage. Your people get the work that needed them all along.

**Nobody hired your IT director to reset passwords. The split gives them their job back.**

SOLUTION BUILDERS CO-MANAGED PRACTICE

# How to prove it to the CFO on one page.

Finance does not buy hours. Finance buys outcomes with a number attached. Put the before and after side by side, price the risk you retired and list the projects that shipped. This page is the template.

### The one page business case

| LINE | HOW TO MEASURE IT | EXAMPLE |
|---|---|---|
| **Hours reclaimed** | Hours per week back, times loaded hourly cost | 3 engineers, 15 hours, 48 weeks: 2,160 hours a year |
| **Downtime avoided** | Downtime hours before and after, times the business cost per hour | 100+ hours a month to near zero, 85 user manufacturer |
| **Tickets** | Monthly volume and time to resolve, before and after | 60% fewer tickets in 90 days |
| **Coverage** | Hours per week with someone actively watching | From 40 hours to 168 |
| **Projects delivered** | Roadmap projects shipped on time versus the prior year | Three in two quarters, after a year of none |
| **Risk retired** | Single points of failure closed, audit findings cleared | From five key person dependencies to zero |

**Lead with the number the CFO already believes**

Finance usually knows what an hour of downtime costs the plant or the billing team. Start there. Reclaimed hours and retired risk are the supporting lines, not the headline.

### Build the case in four steps

1. **Baseline for two weeks.**
   Have the team log time by category: tickets, patching, firefighting, projects, strategy. Expect to be surprised.
2. **Price the hour.**
   Loaded cost for your engineers. Cost per hour of downtime for the business, from finance, not from IT.
3. **Name the risk.**
   Key person dependencies, systems with no night coverage, audits you are not ready for. One plain sentence each.
4. **Report quarterly.**
   The same four numbers every quarter: hours, tickets, downtime, projects shipped. Boring, consistent and persuasive.

**100+**
hours of monthly downtime eliminated at an 85 user manufacturer

**60%**
fewer support tickets within the first 90 days

**90 days**
from kickoff to full transformation, with the internal team still in charge

Sources: PMI, Pulse of the Profession 2020 (11.4% of investment wasted through poor project performance); time split and reclaimed hour figures are illustrative planning assumptions drawn from Solution Builders client engagements; client outcome from a Solution Builders manufacturing client, 85 users.

# Your IT team, amplified.

Solution Builders has worked alongside internal IT teams in Minnesota since 1995. Co-Managed IT is built on the RISE framework and delivered by 50+ engineers, a 24/7 security operations center and tooling your team gets to use too.

**R**

**Resilient**

Backup, business continuity and cloud resilience your team can lean on, tested quarterly.

**I**

**Integrated**

Shared ticketing, documentation and monitoring, so two teams work from one system.

**S**

**Secure**

24/7 security operations, compliance support and incident response alongside your staff.

**E**

**Evolving**

AI and Copilot guidance so your team leads the next wave instead of chasing it.

**01**

### Co-Managed Fit Call

A 30 minute conversation with your IT lead in the room. You leave with a draft ownership matrix and an honest read on fit.

FREE · 30 MINUTES

**02**

### Key Person Risk Audit

Two weeks to inventory credentials, documentation and single points of failure, with a scored report and a 30 day cure.

FIXED FEE · 2 WEEKS

**03**

### Co-Managed IT Program

Your team plus our bench, 24/7 SOC, enterprise tooling and a quarterly review, scoped to the matrix you choose.

MONTHLY · ONGOING

## See what your team could do with 15 hours back.

Book a free Co-Managed Fit Call with a Solution Builders solution architect. Bring your IT lead. No pitch, just a clear read on where a bench would help.

**Book my fit call**

THE SHORT VERSION

# Three things to remember.

If this playbook ends up in a drawer, keep these three ideas. They are the difference between an IT team that is stretched and an IT team that is amplified.

01

**Co managed adds. It does not replace.**

Your team keeps the decisions, the relationships and the keys. The bench adds hours, specialties and a night shift.

02

**One owner per row, in writing.**

Help desk, patching, security, projects, vendors, strategy. Settle ownership before day one and review it every quarter.

03

**Key person risk is a system problem.**

A vault, a runbook library and a bench that knows your network beat hoping nobody ever takes a vacation.

SOLUTION BUILDERS®

START THE CONVERSATION

## www.solutionbuilders.com

(952) 854-8188 · 1550 American Blvd East, Suite 900, Bloomington, MN 55425
Your technology partner since 1995

Book a free assessment

© 2026 Solution Builders, Inc. All rights reserved. Product names and marks are the property of their respective owners. Figures marked illustrative are planning estimates, not guarantees.