entech

INSOURCE VS. OUTSOURCE IT SERVICES

How To Decide Whether To Insource, Outsource, Or Co-manage IT Services

A practical executive guide for mid-market leaders evaluating IT support, cybersecurity, risk, scalability, and business alignment.

Use this guide to answer one strategic question:

What IT operating model gives our business the right level of capability, accountability, scalability, and risk control?

Designed for CEOs, CFOs, COOs, CIOs, IT Directors, Controllers, and operational leaders.

Executive Summary

IT has become too important to manage as a purely back-office support function. It now affects productivity, cybersecurity risk, operational uptime, compliance readiness, customer experience, and the ability to scale.

For many mid-market organizations, the decision is no longer whether IT should be internal or external. The better question is whether the current IT model can support the business over the next 12 to 24 months.

The Core Decision:

The right model is the one that gives the business the best combination of internal knowledge, external expertise, accountability, security maturity, scalability, and executive visibility.

The Three IT Operating Models

MODEL	BEST FIT	STRENGTHS	WATCHOUTS
Fully Insourced IT	Organizations with scale, strong IT leadership, specialized systems, and sufficient budget.	Deep business knowledge, direct control, cultural alignment, and proximity to users.	Can become expensive and fragile if the team lacks specialized depth, coverage, or security maturity.
Fully Outsourced IT	Organizations without internal IT leadership or those needing broader coverage, structure, and accountability.	Access to a broader team, predictable support, standardization, security maturity, and executive reporting.	Requires strong provider selection, clear onboarding, defined expectations, and ongoing governance.
Hybrid / Co-Managed IT	Organizations with capable internal IT that need added depth, cybersecurity, escalation, or after-hours support.	Preserves internal business knowledge while adding capacity, tools, process, and specialized expertise.	Requires clear roles, shared documentation, and a strong operating rhythm between internal and external teams.

When Each Model Makes Sense

The right model depends on business complexity, internal capability, risk profile, leadership expectations, cybersecurity requirements, budget, and growth plans.

If Your Organization...	Most Likely Fit	Why
Has a mature internal IT leader and enough budget to fund multiple specialized roles	Insourced	The business has the scale and structure to support IT internally.
Has no internal IT leadership or relies on one overloaded generalist	Outsourced	A provider can bring process, coverage, documentation, and accountability.
Has a strong internal IT resource but needs security, coverage, or escalation depth	Hybrid / Co-Managed	The internal team stays close to the business while the provider fills capability gaps.
Is growing, adding locations, or preparing for acquisition or exit	Outsourced or Hybrid	Growth increases the need for standards, reporting, risk control, and scalability.
Faces compliance, cyber insurance, or customer security requirements	Hybrid or Outsourced	Specialized security, documentation, and governance support become more important.

The Hidden Cost of Insourcing IT

Many organizations compare outsourcing fees against the salary of one internal IT employee. That comparison is incomplete. A mature internal model requires people, tools, training, management oversight, coverage, cybersecurity, documentation, and risk controls.

Cost Area and Examples to Include in the Comparison

People: Salaries, benefits, recruiting, retention, turnover, management overhead.

Tools: Ticketing, monitoring, endpoint protection, patching, backup, documentation, remote access.

Security: MDR or SOC, email security, identity controls, vulnerability management, awareness training.

Coverage: After-hours support, escalation, vacation coverage, sick coverage, emergency response.

Risk: Downtime, failed recovery, ransomware exposure, compliance gaps, vendor sprawl, documentation gaps.

Key Point:

Insourcing can be the right answer, but only when the business can fund the full IT capability stack, not just one or two generalists.

Where Under-Resourced IT Creates Risk

Under-resourced IT teams usually do not struggle because people are not working hard. They struggle because the model asks too few people to cover too many responsibilities.

- Single points of failure
- Weak identity controls
- Limited executive reporting
- Inconsistent backup testing
- Reactive firefighting
- Slow response times
- Vendor sprawl
- Burnout
- Security gaps
- Delayed projects
- Incomplete documentation
- Compliance readiness issues

THE CO-MANAGED MODEL

Often the Best Middle Ground

For many mid-market companies, the best answer is not replacing internal IT. It is giving internal IT more leverage.

Internal Team May Keep

- Business application knowledge
- Internal stakeholder relationships
- On-site coordination
- Project ownership and business context
- Day-to-day operational knowledge

Provider May Support

- Help desk overflow and escalation
- Endpoint management and patching
- Cybersecurity monitoring and response
- Backup, disaster recovery, and resilience planning
- vCIO, roadmap planning, compliance support, and executive reporting

What Good Co-management Looks Like:

One operating model, clear roles, shared documentation, defined escalation paths, regular governance, and no confusion about who owns what.

Decision Scorecard

Score each area from 1 to 5. A 1 means low concern or current model is working well. A 5 means high concern or current model creates business risk.

Evaluation Criteria	Score 1 to 5	Notes
Internal IT capacity		
Cybersecurity maturity		
Compliance or cyber insurance requirements		
Business growth or multi-site complexity		
Current IT responsiveness		
Documentation quality		
Backup and recovery maturity		
Cloud and Microsoft 365 complexity		
Executive reporting needs		
Tolerance for operational risk		

Total Score	What It Suggests	Recommended Direction
10 to 22	The current model may be sufficient if leadership has good visibility and risk is controlled.	Insourced model may work.
23 to 37	There are meaningful gaps that may require added capacity or expertise.	Evaluate hybrid or co-managed IT.
38 to 50	The current model may be creating operational, security, or scalability risk.	Evaluate outsourced or co-managed IT seriously.

Financial Comparison Worksheet

Use these questions to compare the true cost and value of each model. The goal is not to prove one model is cheapest. The goal is to understand what it costs to create the capability the business requires.

01 How many internal IT employees would be required to provide adequate coverage?

02 What tools, platforms, or security capabilities are missing or underutilized?

03 How much executive time is spent managing recurring IT issues?

04 What would one day of downtime, ransomware impact, or failed recovery cost?

05 What roles are missing today: help desk, network, cloud, cybersecurity, compliance, leadership?

06 What happens when the primary IT person is unavailable?

07 What projects are delayed because IT lacks capacity?

08 What investments will be required over the next 12 to 24 months?

Provider Evaluation Checklist

If outsourcing or co-managed IT is being considered, evaluate providers on operating model maturity, not just tools or ticket response.

Questions to Ask

01. Onboarding

Do they have a documented 30, 60, and 90 day transition process?

02. Documentation

How will they document users, systems, vendors, risks, and ownership?

03. Pricing

What is included, what is excluded, and how are projects or scope changes handled?

04. Cybersecurity

What monitoring, response, identity, endpoint, and incident response capabilities are included?

05. Strategy

Do they provide roadmap planning, budget guidance, and executive reporting?

06. Compliance

Can they support cyber insurance, audits, questionnaires, and control documentation?

07. Governance

How often will they meet with leadership, and what will be reviewed?

08. Service desk

How are tickets prioritized, escalated, measured, and reviewed?

Red Flags When Evaluating IT Providers

Lead only with tools, not business goals

Avoid cybersecurity specifics

Do not provide executive reporting or QBRs

Cannot support compliance or cyber insurance needs

Use vague pricing or unclear inclusions

Do not clarify roles and responsibilities

Cannot explain onboarding

Focus only on ticket response

Cannot define success metrics

Lack a documented transition plan

Executive Questions to Ask Before Deciding

CEO

Can our current IT model support where the business is going over the next 24 to 36 months? Do we understand our biggest technology and cyber risks?

CFO

Do we understand the full cost of our current IT model? Would another model improve predictability, accountability, or risk reduction?

COO

Are technology issues disrupting productivity, service delivery, or customer experience? Are recurring issues being fixed at the root cause?

CIO / IT Director

Where is the team stretched too thin? Which functions should remain internal, and where would outside expertise create leverage?

Risk / Compliance

Are controls documented, backups tested, access reviewed, and incident response plans current?

Final Recommendation

The best IT model is not always fully insourced or fully outsourced. The best model is the one that gives the business the right mix of internal knowledge, external expertise, operational coverage, cybersecurity maturity, executive visibility, and accountability.

For some companies, that means continuing to invest in internal IT. For others, it means outsourcing the IT function to a provider that can bring structure, security, and leadership. For many mid-market organizations, the best answer is a co-managed model that strengthens internal IT without replacing the value it already provides.

> **Leadership Test:**
>
> Can our current IT model support the business we are becoming, or only the business we used to be?

Suggested Next Step

Build Your IT Services Decision Framework

A practical IT Operating Model Assessment can help your leadership team evaluate the current model, identify capability gaps, compare insourced, outsourced, and hybrid options, and determine what model best supports growth, security, accountability, and operational resilience.

The goal is not to force a decision toward outsourcing.
The goal is to choose the model that best fits the business.

Start a Strategy Session