AMPITO

The Co-Managed Infrastructure Manifesto

Redefining the MSP model in networks and cyber security

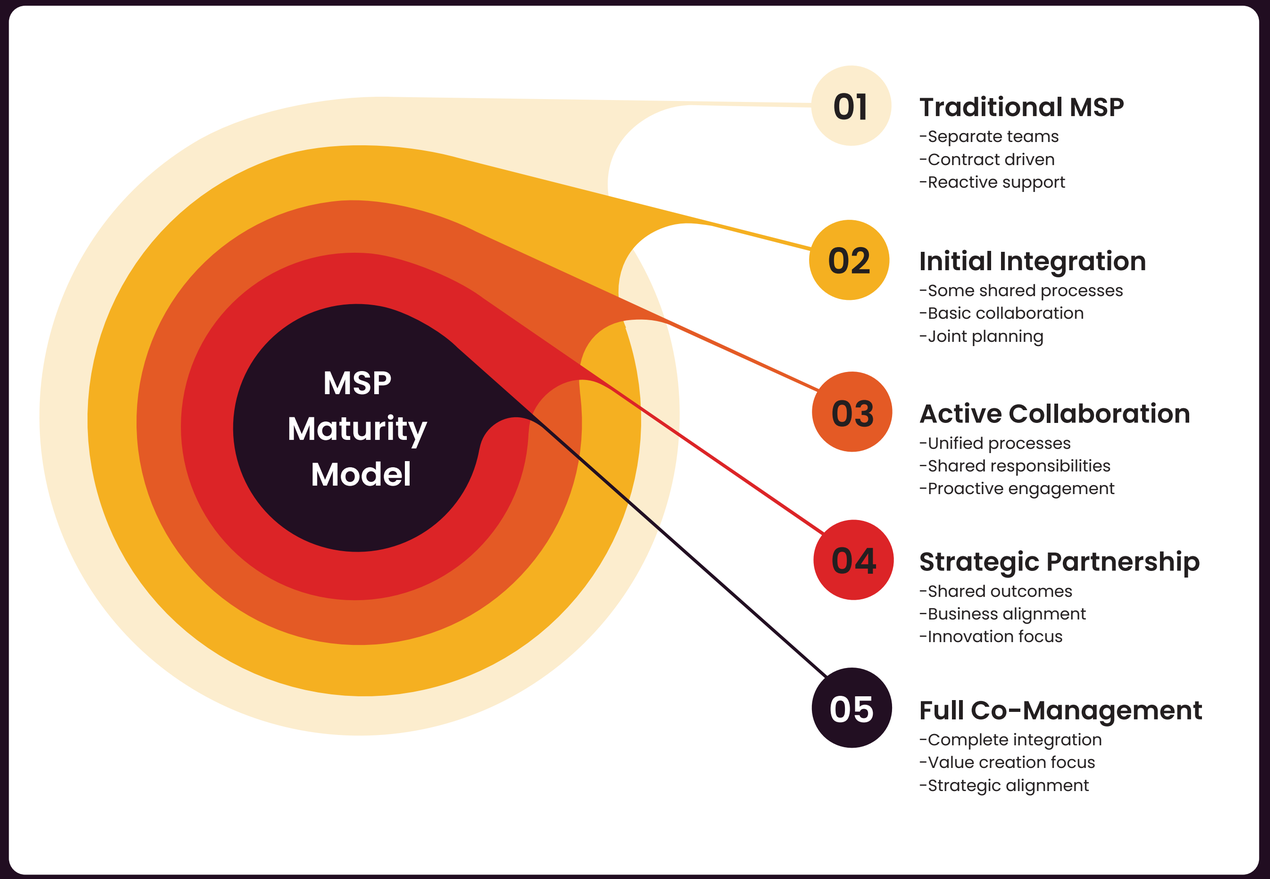

Fig 1.1 The MSP Maturity Model

Executive Summary

The traditional MSP model is no longer fit for purpose in today's complex digital landscape. Cisco's 360 Partner Programme, which will launch on February 1st 2026, reflects the undeniable truth that the future of managed services lies in deep collaboration rather than traditional outsourcing.

This manifesto outlines a fundamental shift from passive service delivery to active co-management of technology infrastructure - where MSPs and client teams work as unified entities, sharing tools, knowledge, and responsibility for business outcomes.

We propose a radical reimagining of the MSP-client relationship, moving beyond traditional SLAs and ticket metrics to focus on business value creation. This co-managed approach combines the deep business knowledge of internal teams with the specialised expertise and broader perspective of MSP partners. Through shared tools, unified workflows, and collaborative decision-making, organisations can maintain technological autonomy while accelerating innovation and reducing operational friction. Our model has demonstrated significant improvements in incident resolution times, change success rates, and overall operational efficiency across multiple sectors.

The transformation to co-managed services requires careful planning and execution. This manifesto provides both the strategic framework and practical steps for organisations to evolve their MSP relationships. From initial assessment through to full implementation, we outline the tools, processes, and organisational changes needed to succeed. By treating technology infrastructure as a living ecosystem rather than a commodity service, organisations can turn their IT operations from a cost centre into a strategic driver of business value.

Contents

ONE

The Crisis of Modern IT

We stand at a critical juncture in technological evolution. Traditional IT MSP models are no longer appropriate for today's complex infrastructures — a system of passive outsourcing that strips organisations of a critical strategic asset: the ability to leverage technology for business advantage.

The era of passive managed services is over. Cisco's 360 announcement merely confirms what has become more evident: the future belongs to collaborative, proactive partnerships between providers and their customers. We recognised this shift in 2018 and pivoted our services around this new paradigm to deliver better results for clients.

The new way forward

Break down the traditional barriers between the MSP and customer teams

Share expertise, tools, and decision-making in real-time

MSPs must transform from service provider to strategic technology partner

Enable customers to maintain control while leveraging our expertise

Build customised hybrid operational models that evolve with business needs

Yet we acknowledge

Organisations cannot afford to be test beds. The transition to co-managed services must be measured and proven. Our role is to:

1. Demonstrate clear benefit and advantage at each step (Operations, support and strategic value)
2. Create flexible engagement models that allow for gradual adoption
3. Protect existing technical abilities, knowledge, skills and intelligence while introducing new capabilities
4. Share risk through transparent metrics
5. Provide concrete examples of value creation through co-management

We don't just preach transformation – we practice it. Every co-managed partnership we build is backed by proven methodologies, established governance frameworks, and measurable business outcomes.

The ideal MSP Co-Managed Model:

Customer

- Hands on
- Day to day control
- Policy change
- Access to reporting and recommendation
- Balance resource limitation

Improved IT reputation for delivering on business initiatives quickly, securely and with a best practice aligned to the organisation.

MSP

- Flexibly plug new tech experience & resource gaps.
- Ensure inherited technical debt doesn't impede progress
- Deliver best practice
- Handle routine work

TWO

IT is not a problem to be solved, but a living ecosystem to be cultivated.

The Fundamental Principles of co-managed infrastructure:

- 1 - Technological Autonomy

- 2 - Collaborative Intelligence

- 3 - Infrastructure as a collective capability

1. Technological Autonomy

We reject the myth of complete outsourcing. The notion that technology operations can be removed from an organisation and handed wholesale to external parties is not just misguided – it can be actively harmful to business growth and innovation. This outdated thinking has led countless organisations down a path of diminished capability and strategic paralysis.

This is one reason why Cisco's new 360 framework emphasises customer-provider collaboration across the entire technology lifecycle, not just at implementation points.

Infrastructure is a living, breathing organism that embodies an organisation's capabilities, aspirations, and competitive advantages. Every server, every network connection, every line of code carries within it the DNA of how an organisation operates, competes, and delivers value. To treat this complex ecosystem as a simple utility is to fundamentally misunderstand its role in organisational success.

Cisco's shift to full-lifecycle engagement mirrors our long-standing approach: deep integration between internal teams and external partners, sharing not just tools but strategic vision and operational responsibility.

In today's digital economy, every technology decision impacts the entire organisational structure - the selection of a cloud platform, the architecture of a network, the choice of security protocols – are not merely technical decisions to be delegated but strategic choices that shape an organisation's future possibilities. They determine not just operational efficiency but competitive advantage, market agility, and your capacity for innovation.

This truth demands a new model of partnership between organisations and their technology providers. One where expertise is shared, decisions are collaborative, and both parties are invested in strategic outcomes.

To separate technology decisions from business strategy is to create artificial boundaries that serve neither the present nor the future.

2. Collaborative Intelligence

The fundamental principle of Collaborative Intelligence demands the breaking of traditional hierarchies of technological knowledge, as concentrated power is wasted power.

Siloing technical expertise creates single points of failure and stifles innovation, and no single entity can possibly maintain cutting-edge expertise across all domains or fully grasp every client's business environment.

The future belongs to those who acknowledge this new reality and build models leveraging diverse sources of expertise.

When internal teams and external partners engage as equals, questioning assumptions and combining diverse perspectives, breakthrough thinking becomes possible. This approach requires new frameworks for interaction, metrics for success, and a mindset shift about technological expertise itself – moving beyond simple client-vendor relationships to create partnerships where knowledge flows freely, challenges are met with collective wisdom, and innovation emerges from combined strengths.

3. Infrastructure as a collective capability

We must change the reductive view of technology as a mere cost centre to be minimised and controlled. This outdated perspective blinds organisations to the true nature of their technology landscape: a generative ecosystem that creates value, drives innovation, and enables transformation. In this organisational DNA ecosystem, every component, every connection, every interaction holds the potential for organisational growth and competitive advantage.

The question is not how to minimise technology costs, but how to maximise its generative potential.

Even the most mundane technical elements carry transformative potential. Each network packet flowing through an organisation's digital nervous system is not merely carrying data – it carries the seeds of organisational transformation.

This vision requires us to move beyond the traditional metrics of cost and efficiency to measure and maximise technology's contribution to value creation. Further driving a new kind of collaboration between business and technology leaders, internal teams and external partners.

THREE

The Call to Action: How it works in practice

What can you do now? Where do you start?

1. Dismantling the False Internal/External Dichotomy

Stop running separate change control boards and start hosting unified technology steering committees. Merge your incident response teams. Create shared Webex channels that connect your network engineers directly with ours.

For example, where you may have a lack of expertise around a new technology such as SASE, your MSP team should be on hand to answer questions, fill skills gaps and provide help with challenges that inhibit digital transformation initiatives.

Merging security operations with their MSPs through unified monitoring systems, ticket queues, and automation platforms, organisations can detect attack patterns in hours rather than days and significantly reduce alert duplication - replacing siloed tools and dashboards with seamless, shared observability.

2. From Service Contracts to True Partnership

Tear up SLA-obsessed contracts that measure the wrong things. Replace them with outcome-based agreements that track business metrics.

For example: Instead of network uptime, measure production line efficiency in your factories. Instead of ticket resolution times, track customer transaction completion rates.

If you need to enable SD-WAN, but have a complex underbelly of telecommunications that had been inherited and built on over several years, we can take on the complexity of managing all of that - from the great switch off, to unpicking billing and managing mobile connectivity.

Create joint innovation groups where both parties plan new capabilities - especially when you're enabling transformation in remote sites outside the HQ. Knowing you have a partner that can manage the underlying complexity around connectivity and security enables digital transformation to happen quickly.

Build outcome success.

3. Real-world Success Requirements

Your process for driving co-managed success:

1. Set up joint operations rooms during major incidents (virtual or physical)
2. Create combined architecture review boards with equal representation
3. Establish shared training programs where teams learn together
4. Build unified project teams with blended leadership
5. Share technology roadmaps and budget planning sessions
6. Create combined security response teams with shared playbooks
7. Implement shared on-call rotations where appropriate

Your MSP should be able to deliver a proactive service model by collaborating on monitoring and observability.

4. Strategic Collaboration in Daily Operations

Replace quarterly vendor reviews with weekly joint strategy & operational review sessions. Embed MSP architects directly in your planning teams.

For one retail client we were able to save them 25% of their renewal fee by removing the need for Returns Material Authorisations (RMA) as we could analyse and tell them upfront what break/fix spares to purchase, which was reinvested in other projects.

Alternatively, another client only had high value engineers that they didn't want on 1st and 2nd line support, so we took that on, and gained efficiency savings of 65%.

Share your business KPIs with us - not just your technical metrics. Example: A manufacturing company can give direct access to their production efficiency dashboards, enabling the MSP to proactively tune infrastructure based on real business impact.

Stop building rigid demarcation points. Instead, create flexible operational zones where responsibilities shift based on needs and capabilities.

When you need help in a specific region we can provide out of hours support in any location. For a healthcare provider, we implemented a tailored solution which included holding stock and deploying engineers in regions where they did not have local IT resources. This approach reduced their average time to fix by over 50%, demonstrating how our adaptable managed service models can deliver tangible results while complementing your internal capabilities.

Example: During Black Friday, a retail company's internal team can focus on customer experience while the MSP dynamically scales their infrastructure. During normal operations, these roles blur and shift. Implement dynamic access controls that adapt to operational needs - not static RACI matrices.

The NHS used this model to reduce change approval times from days to hours. Sharing tools and platforms rather than building separate toolchains.

5. Creating Self-Evolving Systems

Deploy AI-driven observation tools across both environments to spot patterns to enable speedy adaptation to market, commercial and operational changes.

- Build joint automation teams that create shared scripts and workflows
- Implement unified monitoring that learns from both teams' responses
- Create combined DevOps pipelines that auto-optimise based on real usage
- Share configuration management databases to enable automated decision-making
- Build unified incident response playbooks that improve through machine learning

Practical result from this new model

Rationalising client data to give them context about issues. A trade supplies company had 2 to 5 devices per site, all generating alerts - we consolidated and rationalised to enable quicker diagnosis and mitigation. This reduced the number of service tickets by 70%.

70%

service ticket reduction

FOUR

Strategic Imperatives

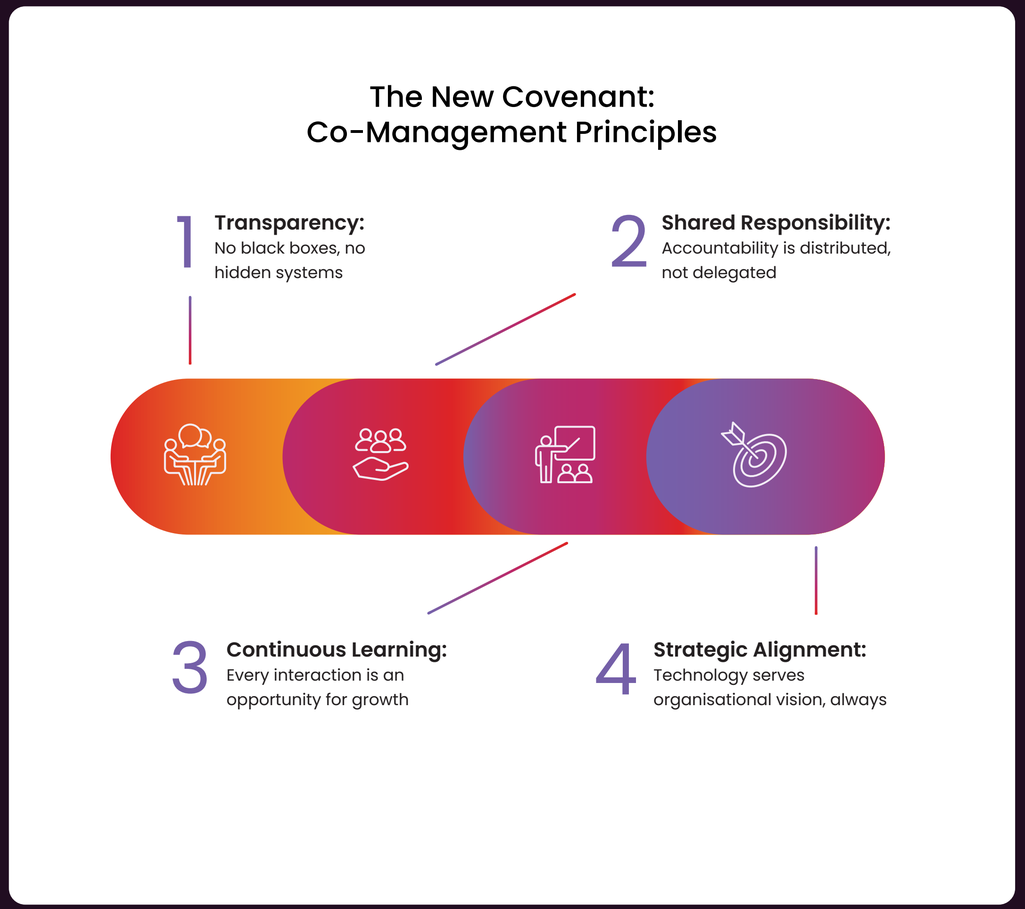

Fig 4.1

For Leadership

Recognise shared technological capability as a core strategic competency

Invest in human technological intelligence

Create organisational structures that embraces inter-organisational complexity

For Technologists

Remove the boundaries between you and your MSP

Develop skills of translation and collaboration

Be architects of possibility, not just maintainers of infrastructure

FIVE

A Practical guide to implementation of a co-managed model using Cisco Technology:

1. Getting started: Audit Your Current Model & identify friction points

Start by documenting every intersection point between internal and external teams. Create a comprehensive interaction map showing where handoffs occur, where decisions are made, and where knowledge is shared or blocked.

For example work to map the organisation by RACI (Who is Responsible, Accountable, Consulted and Informed), which avoids the trap of getting caught up with multiple Proof of Concepts. We worked with a major real estate agent, who had six or seven different connectivity vendors initially, but by working with us they're only dealing with one partner instead of looking at every alert from all of the connectivity providers.

Track for one week: Every escalation, every approval request, every emergency bridge call. Look for patterns: Where do delays consistently occur? Where do miscommunications happen? Which teams are constantly waiting on others?

Document shadow IT practices - they often reveal where official processes are failing.

Purpose/ Need	Visibility & Mapping	Monitoring & Analysis	Communication & collaboration	Security & Control
Team Interaction Mapping	DNA Center Dashboard, Meraki Dashboard, Intersight	AppDynamics Business iQ, ThousandEyes	Webex Analytics, Cisco Spaces Analytics	ServiceGrid (handoffs)
Process Flow Analysis	ThousandEyes, DNA Center	AppDynamics Business iQ, Intersight Metrics	Webex Meeting Analytics, Cisco Spaces Usage Data	Secure Network Analytics
Shadow IT Detection	ThousandEyes, DNA Center	Secure Network Analytics		Umbrella, Secure Endpoint
Cross-Team Operations	DNA Center, Intersight	Full-Stack Observability, AppDynamics	Webex, Cisco Spaces	ServiceGrid
Automation & Integration	DNA Center APIs, Intersight APIs	AppDynamics APIs, ThousandEyes APIs	Webex APIs	Security APIs, ServiceGrid APIs

Fig 5.1 Cisco tools to get you started

2. Practical Actions:

- Review last six months of major incidents - identify where team boundaries delayed resolution
- Map decision rights - highlight where authority is unclear
- Analyse change request pipelines - spot where approvals get stuck
- Review tool access - note where limited visibility impacts performance
- Examine ticket workflows - find redundant handoffs
- Audit communication channels - identify information bottlenecks

Purpose/ Need	Visibility & Mapping	Monitoring & Analysis	Communication & collaboration	Security & Control
Incident Analysis	AppDynamics, ThousandEyes, Intersight	Full-Stack Observability	WebexCisco SpacesDNA Center alerts history	ServiceGridSecureX automation
Change Management	DNA Center, Intersight, AppDynamics	DNA Center Metrics, Intersight Metrics	Webex Spaces	DNA Center APIsIntersight APIs
Ticket Workflow	ServiceGrid, SecureX Dashboards	ServiceGrid Analytics	Webex Spaces	ServiceGridSecureX Integrations
Access Management	ISE Visibility, DNA Center, Meraki Dashboard	ISE Policy Management, DNA Center RBAC	Webex Control HubSpaces Admin Console	ISE APIsDNA Center Access APIs
Communication Audit	Webex Analytics, Spaces Analytics, Intersight	Webex Control HubDNA Center Notifications	Webex (Real-Time) Spaces (Persistent) SecureX	Webex APIsSpaces Webhooks

Fig 5.2 Aligning tools to outcomes.

You can take it one step further and create consolidated tiger teams, between your MSP and your internal people, to integrate some of these actions, such as an architecture review board for example.

Investing in the above collaborative technologies helps you build API-driven, transparent systems that can create real-time shared visibility and enable the development of tools that deliver collaborative management.

Redesigning engagement models to strategically aligned frameworks that define SLAs, setting up joint governance structures and shared metrics of success will ensure that the co-management model works for you.

3. What that path to transition could look like:

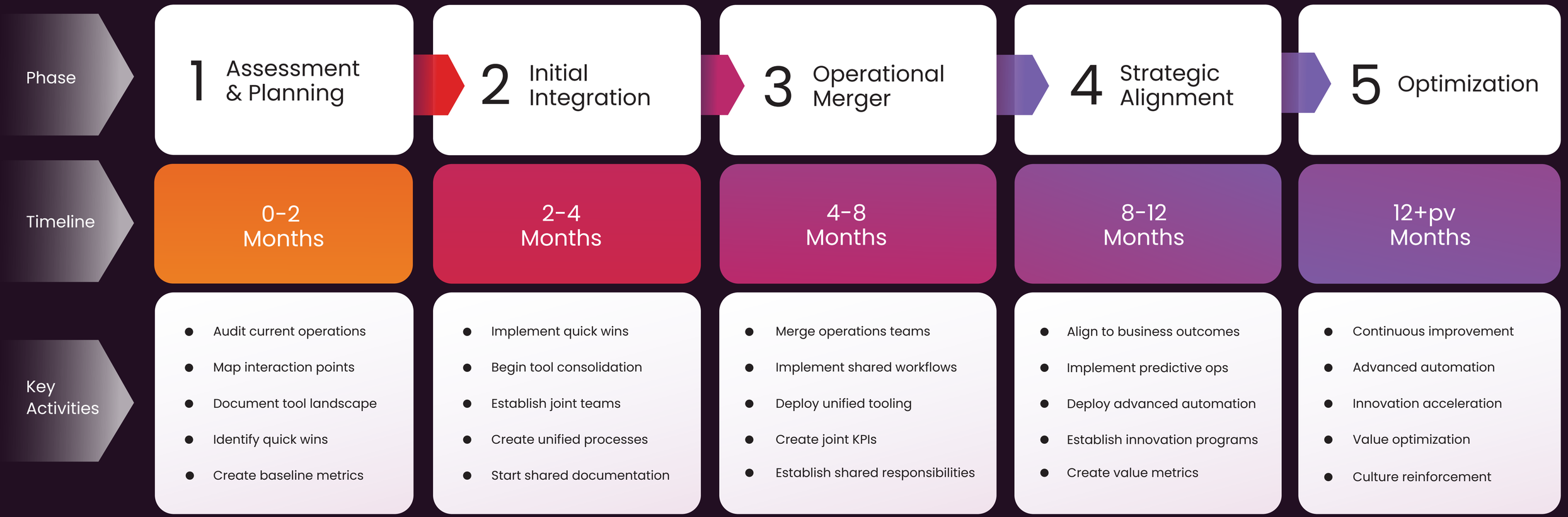

Fig 5.3 Example project phases.

4. Resulting benefits

Benefit Category	1 Financial	2 Operational	3 Strategic	4 Customer Experience	5 Team Benefits	6 Risk Mitigation
Measurable Impact	• 20-30% tool cost reduction • Lower incident costs • Reduced training overhead • Better resource utilisation	• Faster incident resolution • Higher change success rates • Reduced alert noise • Streamlined workflows	• Faster tech adoption • Better risk management • Enhanced innovation • Improved scalability	• Reduced complaints • Better feedback • Higher retention • Improved satisfaction scores	• Reduced burnout • Higher retention • Improved skills • Better engagement	• Fewer critical incidents • Better audit outcomes • Faster recovery times • Enhanced security
Business Value	• More predictable IT spend • Better ROI on technology • Lower operational costs	• Better service delivery • Improved reliability • Enhanced efficiency	• Competitive advantage • Future-proofed operations • Better business alignment	• Stronger relationships • Increased trust • Better business outcomes	• Stronger teams • Better service delivery • Innovation culture	• Business protection • Regulatory compliance • Operational resilience

Fig 5.4 What operational benefits you can expect from a co-managed model

We challenge you

Are you managing technology, or is technology managing you?

Can you transform your infrastructure from a cost centre to a strategic accelerator?

Will you choose technological sovereignty or continued digital colonisation?

SIX

Taking the First Steps: Your Co-Managed Journey

The transition to a co-managed model doesn't happen overnight, but you can begin the journey today. Here's how to get started:

Immediate Actions (Next 30 Days)

- [ ] Schedule a co-management readiness assessment with Ampito designed to achieve quick wins, and to map your current interaction points.
- [ ] Document your primary pain points and friction areas.
- [ ] Begin collecting baseline metrics for current operations.

First Conversation Starters

- [ ] Share your digital transformation goals with Ampito.
- [ ] Discuss where your internal teams feel unnecessarily constrained.
- [ ] Identify areas where you need deeper expertise.
- [ ] Explore opportunities for tool consolidation.
- [ ] Consider joint training and development opportunities.

Remember:

- Your journey will be unique to your organisation
- Focus on outcomes, not just activities
- Build trust through transparent communication
- Celebrate early successes
- Learn and adjust as you progress

The future of IT isn't about outsourcing vs insourcing – it's about creating powerful partnerships that amplify your capabilities while maintaining your technological sovereignty. Your MSP should be ready to evolve with you on this journey, transforming from a service provider to a strategic partner in your success.

Ready to begin?

Contact us to schedule your co-management readiness assessment and take the first step toward technological empowerment.

ampito.com

info@ampito.com

+44 (0)870 352 1001


AMPITO