

TARGET OPERATING MODEL

Sample Company Ltd

Prepared by Managed247 · 8 October 2026

 PREPARED FOR

Jordan Reeves · IT Director · jordan.reeves@example.com

Contents

Part 1 Scope	3
What the model represents and how to read each of the operating-model options.	
Part 2 Executive Summary	4
The model in plain language, followed by the headline ratios and the category breakdown.	
Part 3 Target Operating Model	6
Service-by-service ownership across the capability areas, with a description for every line.	
Service Management Processes	6
Service Desk & Service Delivery	8
Technology Management	10
Patch & Vulnerability Management	12
Cyber Security Management	14
Governance, Risk & Compliance	16
Part 4 Operating the Model	17
The shared services and handoffs to govern, observations worth validating, and next steps.	
Observations & considerations	18
Recommended next steps	19
Part 5 Appendix: Services Not Required	20
Services consciously excluded from scope, recorded so the assessment is auditable.	

Scope

A Target Operating Model (TOM) defines how the IT services that an organisation depends on are owned, delivered and governed. It makes deliberate the choices that are otherwise made by accident: what stays with internal teams, what is partnered out to a managed service provider, what is delivered by a specialist third party, and what is consciously out of scope.

This document captures the operating model selected for Sample Company Ltd across 6 capability areas and 71 applicable services. Each service has been categorised against one of the four operating-model options defined below.

The four operating-model options are:

Internal Team	Owned and delivered by the organisation's own people, tools and processes. Suits services where the in-house team has the capacity, skills and tooling to operate at the required service level.
Managed247	Outsourced to Managed247 as a managed service, with defined SLAs, deliverables and named accountability. Suits services where 24x7 cover, specialist skills or operational scale are needed without growing the internal team.
Co-Managed	Run jointly between the internal team and Managed247, sharing tools and collaborating to deliver the service. Suits services where the internal team needs additional reach, out-of-hours cover or specialist skills without giving up day-to-day involvement.
Other 3rd Party	Delivered by another supplier: typically a vendor, specialist or partner. Captured for completeness so the operating model reflects the full picture of who does what.
Not Required	Not in scope of the operating model. Excluded from headline figures and ownership pies; listed in the Appendix so the assessment is auditable end-to-end.

Executive Summary

THE MODEL AT A GLANCE

Sample Company Ltd's target operating model is a retained IT model with selective partnership. Of the 71 applicable services, 44 (62 per cent) remain with the internal team, 14 (20 per cent) are delivered by Managed247 as managed services, 11 (15 per cent) operate co-managed and 2 (3 per cent) sit with other third-party suppliers.

The partnership is concentrated in Technology Management and Service Management Processes. Services placed with Managed247 include IT Strategy & Technology Roadmap, First Line Service Desk In Hours and Workspace Platform Management (Microsoft 365 / Google Workspace).

The 11 co-managed services in Service Management Processes, Service Desk & Service Delivery, Technology Management, Patch & Vulnerability Management, Cyber Security Management and Governance, Risk & Compliance are where delivery is shared between two parties: each needs a named owner on both sides, shared tooling and an agreed escalation path, and they are set out in Operating the Model below.

1 service is consciously out of scope and recorded in the appendix so the assessment remains auditable; third-party exposure is narrow, at 2 services.

BY THE NUMBERS

71

applicable services

6

capability areas

11

co-managed services

5

cross-party handoffs

HOW TO READ THIS REPORT

Part 3 answers “who runs what” service by service, with a description for every line so the allocation is unambiguous.

Part 4 answers “how the model holds together”: the shared services and handoffs to govern, the observations worth validating, and the recommended next steps.

The appendix records anything consciously excluded, so the assessment stands up to audit end to end.

Executive Snapshot

77% of your IT operation is kept in-house.

Based on 71 applicable IT services across 6 categories.

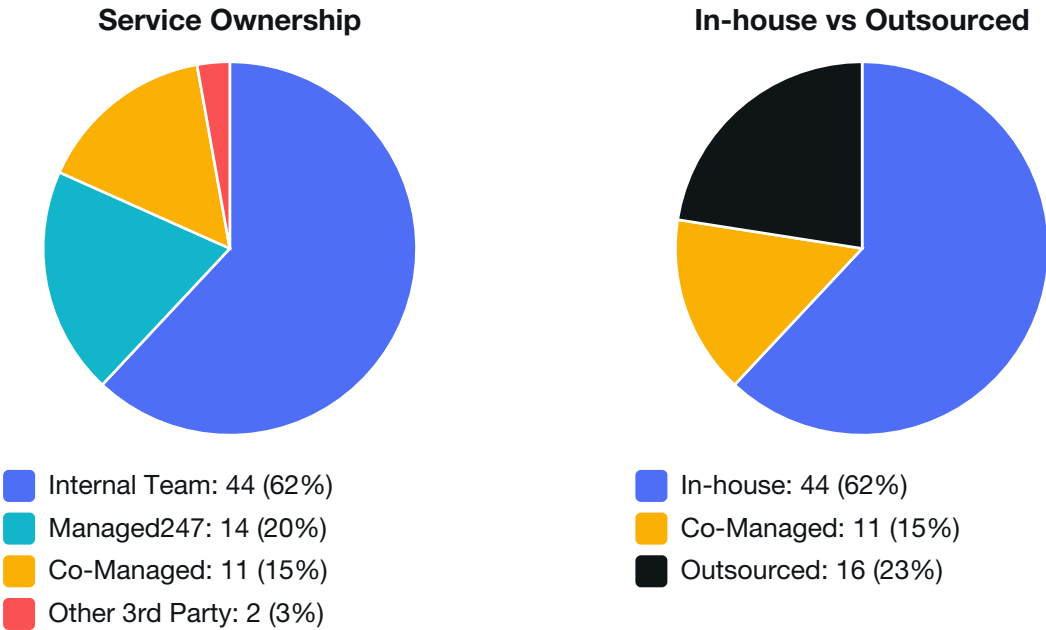
Your Details

Name:	Jordan Reeves	Company:	Sample Company Ltd
Job title:	IT Director	Work email:	jordan.reeves@example.com
Phone:	-	Industry:	Legal / Professional Services
Employees:	101–250	Head office:	Manchester
Users location:	Multi-site (UK only)		

Services Summary

Internal Team 44 / 71 (62%)	Managed247 14 / 71 (20%)	Co-Managed 11 / 71 (15%)	Other 3rd Party 2 / 71 (3%)
---	--	--	---

Services Overview



Category breakdown

Capability area	Internal	Managed247	Co-Managed	3rd Party	Total
Service Management Processes	7	4	2	0	13
Service Desk & Service Delivery	8	1	2	0	11
Technology Management	7	5	2	1	15
Patch & Vulnerability Management	7	0	2	1	10
Cyber Security Management	9	2	2	0	13
Governance, Risk & Compliance	6	2	1	0	9

Service Management Processes

13 services · 7 Internal Team · 4 Managed247 · 2 Co-Managed · 0 Other 3rd Party

Service Management Processes operates a genuinely mixed model: 7 internal, 4 with Managed247 and 2 co-managed across 13 services. The co-managed services here rely on joint delivery, so both sides need named owners and shared visibility of the queue.

Managed247

IT Strategy & Technology Roadmap

Ownership of the IT strategy, technology roadmap and investment plan aligned to business objectives. Provides senior advisory input, architecture direction and annual budget planning through a vCIO or equivalent function.

Internal

ITSM Tooling & Platform

Provision, configuration and ongoing administration of the ITSM platform underpinning the operating model. Includes workflows, integrations and reporting to make process management tangible day-to-day.

Internal

Incident Management

Restoration of normal service operation as quickly as possible after an unplanned interruption, minimising impact on business operations. Covers ticket triage, diagnosis, resolution and post-incident review aligned to ITIL practice.

Internal

Major Incident Management

Coordinated response to high-severity incidents that materially disrupt services or affect multiple users. Provides a dedicated incident manager, executive communications, war-room coordination and post-incident review with corrective actions.

Internal

Request Management

Fulfilment of standard service requests such as access, equipment, software installations and information requests. Operates a service catalogue with automated workflows, approvals and SLA-tracked delivery to keep day-to-day demand off the incident queue.

Internal

Problem Management

Investigation of underlying causes of recurring or major incidents to prevent recurrence and reduce risk. Maintains a problem register, root-cause analyses and a known-error database to drive lasting service stability.

Internal

Change Management

Controlled assessment, approval, scheduling and review of changes to live services to minimise risk and disruption. Operates a Change Advisory Board, change calendar and post-implementation reviews aligned to ITIL.

Managed247

Release & Deployment Management

Planning, packaging and controlled rollout of software releases and infrastructure changes into production. Coordinates technical, business and communications activities to deliver releases predictably with documented rollback paths.

Co-Managed

Knowledge Management

Capture, curation and reuse of operational knowledge to accelerate resolution and shift work left. Maintains knowledge articles, runbooks and FAQ content within the ITSM platform with quality and review cycles.

Service Management Processes (continued)

Internal

Configuration Management (CMDB)

Identification, recording and ongoing maintenance of configuration items and their relationships in a Configuration Management Database. Underpins impact analysis, change risk assessment and accurate asset and service mapping.

Managed247

Asset Management

End-to-end tracking of IT hardware and software assets across procurement, deployment, refresh and disposal. Maintains accurate inventory, ownership, location and lifecycle data to inform spend, risk and compliance decisions.

Managed247

Continual Service Improvement

Structured cycle of measuring service performance, identifying improvement opportunities and delivering measurable benefits. Operates an improvement register and prioritisation model so service quality compounds over time.

Co-Managed

IT Procurement & Licensing

Sourcing, quoting and purchase of hardware, software and subscription licences through approved suppliers. Manages renewals, licence optimisation and warranty registration, feeding accurate data into the asset register.

Service Desk & Service Delivery

11 services · 8 Internal Team · 1 Managed247 · 2 Co-Managed · 0 Other 3rd Party

Service Desk & Service Delivery is led by the internal team, which owns 8 of the 11 services, with First Line Service Desk In Hours under Managed247 and Second Line Service Desk In Hours and Service Reporting & Dashboards under co-managed arrangements. The co-managed services here rely on joint delivery, so both sides need named owners and shared visibility of the queue.

Managed247

First Line Service Desk In Hours

Single point of contact during agreed business hours for all user-reported incidents and requests, providing initial logging, triage and resolution where possible. Targets high first-time-fix rates and a consistent, professional user experience throughout the working day.

Co-Managed

Second Line Service Desk In Hours

Skilled technical support during business hours for tickets that cannot be resolved at first line, covering desktop, application and identity issues. Owns deeper diagnosis and works alongside third line and vendors to restore service.

Internal

Third Line Service Desk In Hours

Subject-matter expert support during business hours for complex incidents and requests across infrastructure, networks, cloud and core platforms. Engages on escalations, problem investigations and technical changes requiring deep platform knowledge.

Internal

First Line Service Desk Out of Hours

Single point of contact outside agreed business hours for incidents and requests, providing logging, triage and initial resolution whenever the in-hours desk is closed. Maintains user experience and service availability through nights, weekends and public holidays.

Internal

Second Line Service Desk Out of Hours

Skilled technical support outside business hours for tickets escalated from first line, covering desktop, application and identity issues. Ensures continuity of deeper diagnosis and resolution capability when in-hours teams are unavailable.

Internal

Third Line Service Desk Out of Hours

Subject-matter expert support outside business hours for complex or critical incidents across infrastructure, networks, cloud and core platforms. Provides on-call expertise for escalations and major incidents requiring deep platform knowledge.

Internal

On-Site Support

Engineer attendance at user, office or data-centre locations for incidents and changes that cannot be resolved remotely. Provides hands-on hardware support, smart-hands services and project assistance as required.

Internal

Multilingual Support

Service desk capability in multiple languages to support globally distributed users in their preferred language. Improves resolution times, user satisfaction and inclusion across international operations.

Internal

Vendor Ticket Escalation

End-to-end management of tickets logged with third-party software, hardware and connectivity vendors on the customer's behalf. Owns the vendor relationship to drive resolution and shield users from multi-supplier complexity.

Service Desk & Service Delivery (continued)

Co-Managed

Service Reporting & Dashboards

Regular and on-demand reporting on service performance, SLA achievement, incident trends and customer satisfaction. Provides accessible dashboards and the reporting packs that underpin the monthly and quarterly service reviews run by the Service Delivery Manager.

Internal

Service Delivery Management

Named account leadership accountable for service quality, governance, customer satisfaction and continual improvement. Runs service reviews, manages risks and improvements and acts as the customer's senior point of contact.

Technology Management

15 services · 7 Internal Team · 5 Managed247 · 2 Co-Managed · 1 Other 3rd Party

Technology Management operates a genuinely mixed model: 7 internal, 5 with Managed247, 2 co-managed and 1 third party across 15 services. The co-managed services here rely on joint delivery, so both sides need named owners and shared visibility of the queue.

Internal

Business Application Support & Maintenance

Support and lifecycle maintenance of in-scope business applications, including configuration, user administration, integrations and minor changes. Coordinates with software vendors for upgrades and incident escalation; routine patch deployment for client-side applications sits under Non-OS Application Patching.

Internal

Endpoint Device Management

Provisioning, configuration, security baselining and lifecycle management of laptops, desktops and other end-user devices. Delivered through UEM tooling to enforce policy, encryption and software currency; phones and tablets sit under Mobile Device Management.

Co-Managed

Mobile Device Management

Enrolment, configuration and security control of corporate and BYOD mobile devices accessing company data. Enforces compliance policies, application management and remote-wipe capabilities to protect data on the move.

Internal

Network Device Management

Configuration, monitoring and lifecycle management of routers, switches, wireless and SD-WAN infrastructure. Delivers reliable connectivity through change-controlled configurations, firmware currency and capacity planning; firewalls and other security appliances sit under Network & Platform Security Management.

Internal

Connectivity Management

End-to-end management of internet and wide-area connectivity, including ISP relationships, fixed lines, broadband, MPLS and resilience links. Covers provisioning, performance monitoring, fault management and supplier coordination so connectivity remains available, fast and predictable; the SD-WAN overlay itself sits under Network Device Management.

Internal

Voice & UC Management

Management of voice communications and the systems that deliver them: IP telephony, contact-centre platforms, conferencing and unified communications services. Includes user provisioning, call-routing configuration, call-quality monitoring and supplier coordination across the voice estate.

Internal

Server, Storage & Infrastructure Management

Operational management of physical and virtual servers, storage arrays and supporting infrastructure across data-centre and edge locations. Includes capacity, performance, patching coordination and lifecycle planning.

Managed247

Data Centre Management

Operational management of data-centre facilities, including space, power, cooling, cabling and physical access. Covers vendor coordination, environmental monitoring and capacity planning for on-premises, hosted and colocated environments.

Technology Management (continued)

Managed247

Workspace Platform Management (Microsoft 365 / Google Workspace)

Administration, hardening and optimisation of the organisation's core workspace platform, covering email, collaboration, file storage and messaging (a Microsoft 365 or Google Workspace tenant). Includes licence assignment, tenant configuration, governance and adoption support.

Managed247

Identity Platform Management

Operation of the identity platform, including users, groups, policies and federation (for example Microsoft Entra ID, Active Directory or Google Cloud Identity). Underpins authentication and lifecycle integration with HR and downstream systems, and is the foundation that every other identity-security control depends on.

Managed247

Public Cloud Management (Azure / AWS / GCP)

Day-to-day operation, governance and optimisation of public cloud environments across Azure, AWS and Google Cloud. Includes landing-zone management, FinOps, tagging and policy enforcement.

3rd Party

Database Management

Administration, performance tuning, backup verification and patching of relational and NoSQL database platforms. Supports application teams with capacity planning, high availability and incident response for data services.

Managed247

Monitoring & Observability

Continuous monitoring of infrastructure, platforms and applications using metrics, logs and traces. Drives proactive detection, faster diagnosis and capacity insight through unified observability tooling.

Co-Managed

Infrastructure Backup Management

Operation of backup, restore and replication capabilities for servers, storage and supporting infrastructure across data-centre and edge locations. Includes scheduled testing, retention management and recovery-time / recovery-point objective reporting against the agreed DR plan.

Internal

Workspace Backup Management (Microsoft 365 / Google Workspace)

Independent backup and restore of workspace data (mailboxes, files, sites and chat) held outside the platform's native retention, for Microsoft 365 or Google Workspace tenants. Protects against accidental deletion and malicious action, and supports long-term retention obligations beyond standard tenant policies.

Patch & Vulnerability Management

10 services · 7 Internal Team · 0 Managed247 · 2 Co-Managed · 1 Other 3rd Party

Patch & Vulnerability Management is led by the internal team, which owns 7 of the 10 services, with macOS Patching under a third-party supplier and Linux / Unix Server Patching and Risk-Based Vulnerability Remediation under co-managed arrangements. The co-managed services here rely on joint delivery, so both sides need named owners and shared visibility of the queue.

Internal

Windows Server Patching

Scheduled patching of Windows Server operating systems within change-controlled maintenance windows. Coordinates pre- and post-patch checks, rollback paths and reporting to maintain compliance with patching cadence policies.

Internal

Windows Workstation Patching

Automated patch deployment for end-user Windows endpoints with phased rollouts and exception handling. Maintains compliance reporting and remediation of non-compliant devices.

3rd Party

macOS Patching

Targeted patch management for Apple endpoints using MDM-driven workflows for OS updates and security patches. Ensures the macOS estate remains current and aligned to corporate security policy.

Co-Managed

Linux / Unix Server Patching

Patch lifecycle management for Linux and Unix server estates including kernel, package and security updates. Coordinates with application teams to schedule reboots and validate post-patch service health.

Internal

Non-OS Application Patching

Detection and deployment of patches for non-operating-system applications such as browsers, runtimes and productivity tools. Closes a major source of exploitable vulnerabilities outside the OS patching scope.

Internal

Firmware & BIOS Patching

Lifecycle management of firmware and BIOS updates for endpoints, servers and storage hardware. Addresses hardware-level vulnerabilities and stability issues that operating-system patching alone cannot resolve; network device firmware sits under Network Device Patching.

Internal

Network Device Patching

Controlled firmware and software updates for routers, switches, firewalls, wireless controllers and load balancers. Coordinates change windows, configuration backups and post-patch validation.

Internal

Emergency & Zero-Day Patching

Rapid response process for critical zero-day and out-of-band vulnerability disclosures. Provides expedited assessment, communications and remediation outside standard patching cycles to contain emerging risk.

Internal

Vulnerability Scanning

Authenticated and unauthenticated scanning of servers, endpoints and network devices to identify known software vulnerabilities; cloud configuration drift sits under Cloud Security Posture Management. Produces prioritised findings to drive remediation activity and demonstrate compliance.

Patch & Vulnerability Management (continued)

Co-Managed

Risk-Based Vulnerability Remediation

Risk-prioritised remediation programme that aligns vulnerability fix timescales to severity, exploitability and asset criticality. Operates measurable SLAs and dashboards for board-level assurance.

Cyber Security Management

13 services · 9 Internal Team · 2 Managed247 · 2 Co-Managed · 0 Other 3rd Party

Cyber Security Management is led by the internal team, which owns 9 of the 13 services; the remaining 4 services are split across the other operating-model options. The co-managed services here rely on joint delivery, so both sides need named owners and shared visibility of the queue.

Internal

Security Event Monitoring (SIEM)

24/7 collection, correlation and analysis of security events across the estate via SIEM tooling. Detects threats, supports investigations and provides audit-ready security telemetry.

Internal

Managed Detection & Response (Endpoints)

Continuous monitoring and response to threats on endpoints using EDR/XDR tooling and analyst expertise. Includes threat hunting, containment and incident handling for compromised devices.

Co-Managed

Identity Threat Detection & Response (ITDR)

Detection and response to identity-based attacks such as credential theft, MFA fatigue and privilege abuse. Protects the identity plane, which underpins access to all business systems.

Internal

Access Management (SSO / MFA / Conditional Access)

Design and operation of single sign-on, multi-factor authentication and conditional access policies across business applications. Governs joiner, mover and leaver access so the right people hold the right access at all times.

Internal

Privileged Access Management (PAM)

Control, monitoring and just-in-time elevation of privileged accounts using PAM tooling. Reduces standing privilege, protects high-value access and supports audit and compliance requirements.

Internal

Information Protection & Data Loss Prevention

Classification of sensitive information and enforcement of policies preventing inappropriate disclosure or movement of data. Combines tooling, policy and user education to protect data on endpoint, email and cloud.

Internal

Network & Platform Security Management

Operation of firewalls, NAC, IDS/IPS and security configuration of network and platform components. Maintains a hardened, well-segmented foundation for the wider estate.

Internal

Email & Web Security Management

Protective controls for inbound and outbound email and web traffic, including anti-phishing, anti-malware and content filtering. Closes the most common attack vectors for ransomware and credential theft.

Managed247

Cloud Security Posture Management (CSPM)

Continuous assessment and remediation of cloud configuration risks across IaaS and PaaS environments. Identifies drift from secure baselines and benchmarks (CIS, NIST) with prioritised remediation.

Managed247

Security Incident Response (IR Retainer)

On-call incident response capability with defined SLAs for declared security incidents that exceed the routine containment handled under Managed Detection & Response. Includes pre-agreed runbooks and forensic readiness to shorten time-to-respond.

Cyber Security Management (continued)

Co-Managed	Phishing Simulation Regular simulated phishing campaigns to assess and improve user resilience to social-engineering attacks. Provides baseline metrics, targeted follow-up training and reporting on susceptibility trends.
Internal	Cyber Awareness Training Programme of role-based security awareness training for all users covering current threats, policies and safe behaviours. Builds a security-conscious workforce as a measurable layer of defence.
Internal	Penetration Testing Scheduled testing of external, internal and application estates by qualified testers to identify exploitable weaknesses beyond automated scanning. Provides prioritised findings, retest verification and evidence for Cyber Essentials Plus, ISO 27001 and customer assurance.

Governance, Risk & Compliance

9 services · 6 Internal Team · 2 Managed247 · 1 Co-Managed · 0 Other 3rd Party

Governance, Risk & Compliance is led by the internal team, which owns 6 of the 9 services, with Regulatory Compliance (GDPR / NIS2 / PCI DSS) and Policy & Standards Management under Managed247 and Audit Support & Evidence Management under a co-managed arrangement.

Internal

Information Security Governance (ISO 27001 / SOC 2)

Governance of an information security management system aligned to ISO 27001, SOC 2 or equivalent frameworks. Includes policy, controls, internal audit and management review cycles.

Internal

Cyber Essentials / Cyber Essentials Plus

Preparation, implementation and certification support for the UK Cyber Essentials and Cyber Essentials Plus schemes. Demonstrates baseline cyber hygiene to customers, regulators and insurers.

Managed247

Regulatory Compliance (GDPR / NIS2 / PCI DSS)

Operational compliance support for relevant regulations such as GDPR, NIS2, PCI DSS and sector-specific frameworks. Maintains evidence, control mappings and remediation plans against in-scope obligations.

Internal

Risk Management & Risk Register

Identification, assessment, treatment and monitoring of information and operational risks via a maintained risk register. Provides a forum for risk acceptance, escalation and board-level reporting.

Managed247

Policy & Standards Management

Development, review and lifecycle management of security and IT policies, standards and procedures. Ensures policies remain current, communicated and demonstrably enforced.

Co-Managed

Audit Support & Evidence Management

Coordination and support for internal and external audits, including evidence collation, control walkthroughs and finding remediation. Maintains an evidence library to reduce audit fatigue.

Internal

Business Continuity & Disaster Recovery Planning

Development and maintenance of business continuity and disaster recovery plans, including business-impact analysis, RTO / RPO definition and exercising. Provides assurance the business can withstand and recover from disruption.

Internal

Supplier & Third-Party Risk Management

Onboarding due diligence, ongoing assurance and risk management of third-party suppliers and SaaS providers. Maintains a supplier register with risk ratings, certifications and contractual security clauses.

Internal

Security Leadership (vCISO)

Named senior security leadership accountable for security strategy, risk posture and board reporting. Directs the control set operated across the security and compliance services through a vCISO or equivalent function.

Operating the Model

An operating model succeeds or fails at its boundaries. This section sets out where Sample Company Ltd's model depends on more than one party: the co-managed services that rely on joint delivery, and the service chains that hand off between different owners.

Co-managed services: where delivery is shared

Service Management Processes: Knowledge Management; IT Procurement & Licensing.

Service Desk & Service Delivery: Second Line Service Desk In Hours; Service Reporting & Dashboards.

Technology Management: Mobile Device Management; Infrastructure Backup Management.

Patch & Vulnerability Management: Linux / Unix Server Patching; Risk-Based Vulnerability Remediation.

Cyber Security Management: Identity Threat Detection & Response (ITDR); Phishing Simulation.

Governance, Risk & Compliance: Audit Support & Evidence Management.

Each of these needs a named owner on both sides, a shared view of the queue, and an agreed tie-break when priorities differ.

Cross-party handoffs

1 The in-hours service desk

The in-hours service desk runs across more than one owner: first line under Managed247, second line under a co-managed arrangement and third line under the internal team. Define the handover points, ticket flow and escalation path explicitly so nothing falls between the parties.

2 The vulnerability pipeline

The vulnerability pipeline runs across more than one owner: scanning under the internal team and risk-based remediation under a co-managed arrangement. Define the handover points, ticket flow and escalation path explicitly so nothing falls between the parties.

3 The detect-to-respond chain

The detect-to-respond chain runs across more than one owner: monitoring (SIEM) under the internal team, managed detection and response under the internal team and incident response under Managed247. Define the handover points, ticket flow and escalation path explicitly so nothing falls between the parties.

4 The identity stack

The identity stack runs across more than one owner: the identity platform under Managed247, access management under the internal team and privileged access under the internal team. Define the handover points, ticket flow and escalation path explicitly so nothing falls between the parties.

5 Backup

Backup runs across more than one owner: infrastructure backup under a co-managed arrangement and workspace backup under the internal team. Define the handover points, ticket flow and escalation path explicitly so nothing falls between the parties.

Observations & Considerations

These observations are derived from the shape of the model alone. None is a verdict; each is a question the board can settle in minutes if the answer is already known.

1 Out-of-hours cover is retained while in-hours first line is partnered

Daytime first-line contact sits outside the internal team, yet overnight and weekend tiers remain in-house. That inverts the more common pattern of extending cover through a partner when the internal team is off shift, and is worth validating: it implies an internal on-call rota, with its associated cost and resilience demands, alongside a partnered day service.

2 Security ownership is spread across several parties

Cyber security services are split across 3 operating-model options. Distributed security ownership can work well, but it raises the coordination overhead during an incident; the detect-to-respond chain in particular should have a single agreed commander and a rehearsed escalation route.

3 A high proportion of the model is co-managed

11 services operate joint delivery. Co-management offers reach without surrendering involvement, but each shared service carries governance overhead: named owners, shared tooling and a clear tie-break. At this concentration the governance cadence deserves explicit board attention.

4 Strategy is partnered while delivery remains in-house

IT Strategy & Technology Roadmap sits with Managed247 while most delivery remains internal. This works well where the advisory cadence is strong; agree how strategic direction flows into the internal delivery teams and how often the roadmap is reviewed together.

Recommended Next Steps

1 Validate the target against current state

Walk each category with the service owners and confirm where today's delivery differs from this target. The gap list that falls out is the transition backlog.

2 Prioritise and phase the transitions

Sequence the moves by risk and dependency rather than by category order; changes to the service desk and security chains are usually phased first because they touch every user and every incident.

3 Define the shared services precisely

For each of the 11 co-managed services and the 5 cross-party handoffs identified in Operating the Model, agree named owners on both sides, the tooling both parties work in, and the escalation route in writing.

4 Set the governance cadence

Put the operating model on a standing agenda: monthly service reviews at delivery level and a quarterly executive review of the model itself, with the ownership ratios in this report as the baseline.

5 Revisit the model on a cycle

Rerun this assessment every six to twelve months, or on any material change such as an acquisition, a platform migration or a significant incident, and compare the result against this baseline.

Managed247 would be glad to walk this model through with you and your board. Contact hello@managed.co.uk to arrange it.

Services Not Required

1 service marked Not Required, listed below by category. These are excluded from the headline figures, pie charts and per-category pages.

Service Management Processes

Project & Change Delivery

Scoped delivery of IT projects such as migrations, upgrades, office moves and new-service introductions outside day-to-day run scope. Provides project management, engineering resource and structured handover into live service.

Marking a service Not Required is itself an operating-model decision. Revisit these exclusions whenever the model is reviewed: growth, regulation or incident experience often brings excluded services back into scope.