

Managed Services Use Case

Tenant Care, Endpoint Care, Backup and Recovery

This example shows how Virtus Group transitions from CPS uplifts to steady-state MS with SLAs/SLOs, evidence, and continuous improvement.

Managed Services Catalogue (14 offerings)	
- Tenant Care (M365)	- Vulnerability and Patch Management
- Endpoint Care	- Email and Domain Protection (Managed)
- Backup and Recovery (Managed)	- Cloud Spend Guardrails (Managed)
- Identity and Access Operations	- Managed Infrastructure
- Network Security Management	- Managed Network
- Managed Cloud	- CAB-as-a-Service
- Safe Web and DNS (Managed)	- PMaaS (Programme or PMO-as-a-Service)

Scenario (illustrative)

A NZ public sector entity of ~1200 users adopts Managed Services after CPS uplifts. We import accepted runbooks and baselines, define SLOs, and integrate with CAB and the change calendar.

Onboarding and handover (Weeks 0 to 4)

- Import CPS runbooks, baselines, access matrices, and role cards.
- Confirm scope, SLAs and SLOs, and KPIs such as incident response and closure, patch compliance, and restore success with RTO and RPO.
- Establish SPOC, escalation ladder, and multi vendor RACI. Align CAB windows and the change calendar.
- Set prerequisites: MoJ or equivalent vetting, least privilege access, MDM controls, and logging destinations.

Operate and improve (steady state)

- Tenant Care: CA and MFA hygiene, risky OAuth and inbox rule monitoring, DLP and labels upkeep, external sharing governance.
- Endpoint Care: patch and vulnerability cadence with an exceptions register, EDR policy hygiene, configuration drift watch.
- Backup and Recovery: enforce immutability, run quarterly restores with evidence, record achieved RTO and RPO.
- Shared service tooling: Decision Log and RAID, change records with rollback plans, ticket queues integrated.

Governance and reporting

- Monthly service review: SLA and SLO performance, incidents and changes, restore evidence, risks and issues, and a live Service Improvement Plan with owners and dates.
- Quarterly: trend analysis and control review, optional tabletop exercise for BC or DR or incident.
- NZ privacy and safety: OPC serious harm threshold and CERT NZ cues in breach response, and a PCBU and H and S safety gate for field or OT contexts.

Multi vendor collaboration

- Coordinated workflows via RACI and a named SPOC, shared evidence, joint change rehearsals and backout plans, and supplier notice windows honoured.

Expected outcomes

- Mailbox hygiene improves and phish related inbox rule incidents trend down.
- Backups are provably recoverable: quarterly restores succeed and achieved RTO and RPO are recorded.
- Patch compliance reaches at least 95 percent within policy windows and critical vulnerability exposure windows shrink.
- Monthly reporting and a closed loop SIP demonstrate continuous improvement.

Links for assessors

Managed Services overview: <https://cdn.virtusgroup.co.nz/resources/services/managed/index.html>

IT Service Packages (tiers): <https://cdn.virtusgroup.co.nz/resources/services/packages/packages.html>

Security and Assurance Index: https://cdn.virtusgroup.co.nz/resources/security/assurance/index/VirtusGroup_Security_Assurance_Index_v1_5.html