



IBM I MANAGED SERVICES . WHITEPAPER

One Retirement Away From a Problem

The pool of experienced IBM i administrators is shrinking. That creates an operational risk most organizations never put a number on. A phased, remote managed-services model closes it without adding headcount.

Prepared by Jeff Grubb, Clear Technologies

Audience IBM i / Power operations and IT leadership

Classification Client-facing

IBM Platinum Business Partner

CLEAR TECHNOLOGIES

01 The risk isn't your system. It's the person who knows it.

Most IBM i shops are not one hardware failure away from a bad quarter. They are one retirement away from it. The platform is famously durable. Boxes run for a decade, and OS releases outlive the projects that once justified them. The expertise that keeps those boxes durable is far less permanent. That gap between resilient technology and fragile knowledge is the real exposure, and it seldom appears on a risk register until the administrator who understood the environment has already left.

The workforce that runs these systems is aging, and the bench behind it is thin. Much of what keeps an IBM i environment healthy lives in one administrator's head: which nightly jobs actually matter, which message queue is the early warning, how the save really runs on the third Sunday when the window is tight. A resignation, a health event, or a retirement that moves up with little notice takes all of that context out the door at once. What the organization loses is less a headcount than an operating manual it never wrote down. The scramble that follows looks the same every time. There is no baseline, no runbook, and no confident answer at 2 a.m. to the one question that counts: whether last night's save can actually be restored.

2 service tiers, scaled to how you're already staffed: monitoring only, or full remote administration	4 governed phases from onboarding to steady-state, so support never begins on an unknown environment	0 additional full-time hires required to put senior IBM i coverage in place
---	--	---

This paper makes a straightforward case: the succession problem is best solved **before** it becomes an incident, by transferring day-to-day IBM i administration to a remote team that documents the environment, watches it on a defined cadence, and reports on it to your stakeholders. Clear Technologies delivers that as two service tiers, entered through a phased engagement designed to protect you from carrying forward unknown risk.

02 “Just hire another admin” is the answer that keeps not working.

The obvious response to a departing expert is to hire another one. It is a reasonable instinct, and often the correct one. But hiring fills the empty seat without touching the deeper problem, which is how much of the operation depended on a single person in the first place.

Keeping IBM i knowledge in-house has genuine advantages: proximity, control, and institutional memory that builds over years. The constraint is supply. Experienced administrators are scarce, expensive, and slow to bring up to speed, so a single hire tends to rebuild the same single point of failure the organization was trying to remove, now with a six-month ramp in front of it. While that hire gets up to speed, lean teams cover critical administration with whoever is available. That holds until the week it doesn't, and the timing of that week is rarely something anyone controls.

A better question is what the coverage actually has to guarantee. Backups should be verified, not just reported as complete. Security exposures should be reviewed on a schedule rather than surfaced by an audit finding. PTF posture should stay current instead of quietly falling a year behind. And someone who has documented how the environment works should be accountable for keeping it that way. When that coverage is delivered as a service instead of resting on one person, it gains a practical kind of durability. It does not retire, take vacation during an incident, or resign with two weeks' notice.

The distinction that matters

A backup process is only complete once a restore has actually been demonstrated. Confirming that a save job finished tells you the job ran; it does not tell you the data can be recovered. Closing that gap, along with the security, PTF, and documentation gaps beside it, is the substance of the work.

03 Two tiers, scaled to how you're already staffed.

Coverage should meet a team where it is thin rather than force an all-or-nothing decision. Clear Technologies offers two remote options. The second is a superset of the first, so moving up a tier adds scope without unwinding anything already in place.

OPTION 1

Monitoring & Operational Support Services

Proactive monitoring and responsive operational support, without adding headcount.

- **Daily** checks: system health, disk & storage, jobs & subsystems, message queues, backup verification, critical applications, security quick checks.
- **Weekly** operational maintenance: log & error review, spool-file cleanup, temporary-storage growth, user-profile activity, communications & network services.
- Delivered as a **monthly retainer plus T&M**; remediation performed under applicable T&M terms when authorized.

Best fit: teams needing expert monitoring, visibility, and responsive support for their IBM i environment.

OPTION 2 · EVERYTHING IN OPTION 1, PLUS

Managed Remote Administration Services

Comprehensive remote administration and lifecycle planning. Effectively your fractional senior IBM i administrator.

- **Monthly** preventative maintenance: PTF / patch posture, security & compliance review, backup & recovery audit, storage & growth planning, journal & database maintenance.
- **Quarterly** deeper review: DR / HA readiness, performance & capacity, configuration, user-access & role review.
- **Annual** strategic planning: full DR test, OS-upgrade & hardware roadmap, licensing & compliance review.
- Backed by a **Monthly Status Checkpoint Call** with your team.

Best fit: teams wanting a comprehensive, fully managed model with reduced administrative burden.

What each tier is worth

Availability

Proactive monitoring and early issue identification catch conditions before they become outages.

Reduced risk

Backup, security, storage, system, and job health reviewed on a defined, accountable cadence.

Governance

Recurring security, compliance, and access reviews strengthen administrative discipline.

Lifecycle foresight

Proactive planning for OS upgrades, hardware, and capacity, so end-of-support dates never arrive as a surprise.

04 Support that starts from a documented baseline.

The engagement is deliberately phased. Responsible long-term management depends on first understanding the current state of the environment: its backup recoverability, its security posture, its monitoring maturity, and the support procedures already in place. The model works toward steady-state support rather than assuming it from day one.

PHASE 0

Onboarding, Scope & Access Setup

Confirm the systems, LPARs, and boundaries in scope; validate secure remote access, authentication, and service-account standards; establish escalation contacts, maintenance windows, approval authorities, and change control.

PHASE 1

Assessment & Operational Baseline

A structured, fact-based review of system health, security, backup/recovery, PTF posture, performance, and monitoring readiness. It delivers findings, a risk-ranked register, a remediation roadmap, and a go/no-go recommendation for steady-state.

PHASE 2

Remediation, Stabilization & Procedure Development

Address prioritized findings, close high-priority gaps, and build the repeatable procedures that reliable day-to-day administration depends on: backup and recovery, security review, PTF maintenance, health checks, and escalation.

PHASE 3

Ongoing Managed Remote Administration

Recurring administration, health checks, monthly service reporting, and periodic reviews. This phase begins only once critical risks are remediated or formally accepted, monitoring is active, and backup visibility is established.

Why gates, not a handoff

Phase 3 does not inherit unresolved issues. Steady-state support begins only once the environment is documented, monitored, and stable enough to sustain it. That sequencing is what keeps an organization from paying to carry forward risk it cannot yet see.

05 The recurring administration model, at a glance.

The following represents the recommended recurring model under Managed Remote Administration. Final checks, thresholds, and escalation rules are confirmed during assessment and stabilization.

Cadence	Representative activities
Daily	System health & status; disk & storage; jobs & subsystems; message queue review; backup verification; critical application checks; security quick checks.
Weekly	System logs & error trends; spool-file cleanup; temporary-storage growth; user-profile & activity review; communications & network services.
Monthly	Apply IBM PTFs / confirm patch posture; security & compliance review; backup & recovery readiness audit; storage & growth planning; journal & database maintenance; Monthly Status Checkpoint Call.
Quarterly	Disaster Recovery / HA review; performance & capacity review; system configuration review; user-access & role review.
Annual	Full disaster-recovery test; OS-upgrade & hardware roadmap; licensing & compliance review.

Where the OS ends and the application begins

These services support the IBM i operating environment and related administration. Application development, functional support, and business-process ownership sit outside the scope unless added by separate written agreement. That boundary keeps accountability clear on both sides.

Whether the risk is on your radar is worth fifteen minutes.

The next step is a short conversation, not a commitment. Fifteen minutes is enough to review how IBM i administration is covered today and to give an honest read on whether a monitoring-only or fully managed model would close a gap before it becomes an incident. If that review confirms the current coverage is already sound, that is a useful thing to establish deliberately instead of finding out during an outage.

Jeff Grubb · Clear Technologies · IBM Platinum Business Partner



Prepared by Clear Technologies for evaluation of IBM i Managed Services. Service scope, monitoring thresholds, service levels, response targets, and commercial terms are defined in the applicable Statement of Work, Managed Services Agreement, or Order Form. This document is client-facing and describes recommended service models; final checks, frequencies, and escalation rules are confirmed during onboarding and assessment.