M-powered

The Co-managed IT Advantage for Airports

Is your back-of-house IT network up to the same standards as your front-of-house passenger experience?

Executive summary

Airports are navigating a perfect storm. Cyber risk is rising, regulatory expectations are expanding, back-of-house systems are aging, and staffing is stretched. Many airports invest heavily in the front-of-house experience, yet an airport's livelihood depends on what passengers cannot see.

Co-managed IT solutions can enable airport leaders to:

- Gain expert IT staff and services on an as-needed and on-demand basis.
- Shift work from reactive to proactive.
- Build a compliance posture you can prove.

The result is lower cyber risk, better network uptime, and a smoother experience for passengers, tenants, and staff.

Introduction

Airports pour energy into what travelers see, but reliability and trust are mostly decided behind the scenes. This white paper explains why more airports are adopting a co-managed IT operating model and how it strengthens safety, compliance, and day-to-day performance without sacrificing control.

Co-managed IT is a true partnership. **Your team determines strategy and keeps the keys, while a specialized partner provides depth, coverage, and operational discipline.** This means continuous monitoring, incident readiness, lifecycle planning, and evidence that stands up to audits.

The co-managed model expands your capabilities where it matters most. **It fills hard-to-hire skill gaps, accelerates project readiness, and frees your people to focus on strategic work instead of firefighting.** Whether you need to manage Wi-Fi, vulnerability management, OT and building-systems segmentation, backup and disaster-recovery testing, or help desk surge capacity, co-managed support scales with your goals and your seasons.

M-powered

The Challenges: Risks, regulations, and staffing

Real incidents, real impact.

In 2024, the Port of Seattle reported that about 90,000 individuals were affected by a ransomware breach that touched port and airport-adjacent systems. In September 2025, a ransomware attack against a third-party aviation software provider disrupted check-in and baggage systems at European hubs including Heathrow, Brussels, and Berlin, forcing manual workarounds and causing delays and cancellations.

Regulation with real teeth.

Airport operators must maintain an Airport Security Program under 49 CFR Part 1542. Since March 2023, TSA has also required certain airport and aircraft operators to implement performance-based cybersecurity measures with approved implementation plans. Regulators and boards increasingly expect proof, not promises.

Safety culture also belongs behind the scenes.

The FAA's Safety Management Systems rule for many Part 139 airports formalize the mindset of find risk, reduce risk, and verify. Applying that discipline to back-of-house technology helps leaders demonstrate control and continuous improvement.

Distributed governance, uneven maturity.

The United States has 435 independent airport authorities and commissions, alongside many city, county, and state-operated airports. A repeatable operating model is essential.

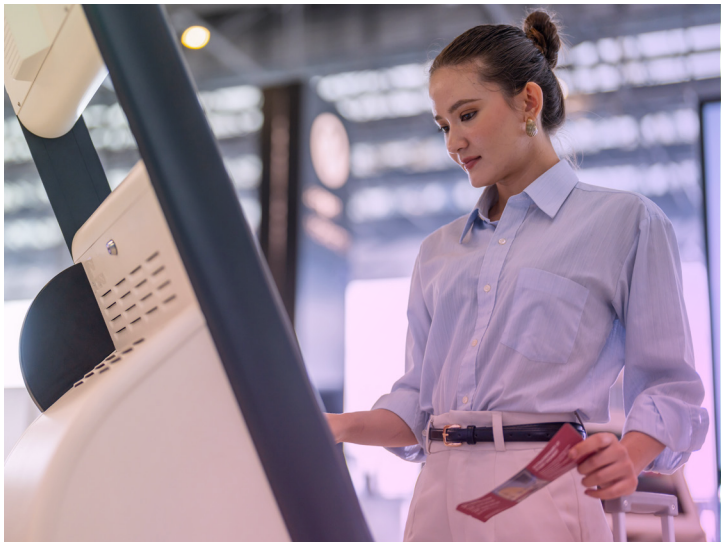
The solution: Why co-managed IT works in airports

Co-managed IT turns policy into daily practice. It builds the routines and evidence that keep airports compliant and resilient, while scaling up or down with seasons and projects. Here is what that looks like in real operations.

- **Operational support.** Always-on monitoring, clear escalation paths, and root-cause analysis reduce noise and catch issues early. This steadies day-to-day operations and frees staff time for higher-value work.
- **Project momentum.** Refresh cycles, Wi-Fi 6E upgrades, segmentation, and cloud initiatives stay on schedule. A co-managed partner brings the bandwidth, playbooks, and specialists to execute predictably, even during peak periods.
- **Cybersecurity confidence.** A reliable vulnerability and patch cadence tested incident response, and audit-ready documentation make compliance with TSA requirements and 49 CFR Part 1542 practical and provable.
- **Specialized expertise.** From NAC and Zero Trust to OT and building-systems isolation, hard-to-hire skills are available on demand without long recruiting cycles.
- **Smarter spending.** Proactive operations beat break-and-fix. Airports avoid emergency outages, overtime, and late-stage rebuilds that cost more than steady discipline.
- **Better passenger and tenant experience.** Fewer disruptions and faster resolution translate into smoother journeys, stronger tenant confidence, and a better reputation with airlines and partners.

Bottom line:

Co-managed IT strengthens your operating model so protections and proof are produced every day, not just during audits.



What co-managed looks like with MGT

You keep the keys. We help you operate, protect, modernize, and support the environment in a measurable way.

Operate

With MGT, you can achieve 24/7/365 monitoring and response with defined service levels, clear escalation paths, performance baselines, and executive reporting. Routine issues are handled before they become incidents, and you see trend data that informs decisions.

Protect

Vulnerability management on a reliable cadence, patch management that does not slip, identity and network access controls, and logical segmentation for passenger, staff, tenant, and OT networks. We prepare incident response, can act as a virtual CISO when needed, and assemble evidence packs aligned to TSA's 2023 cybersecurity requirements and 49 CFR Part 1542.

Modernize

Planning and delivery for Wi-Fi 6 and 6E, switch and firewall lifecycle management, cloud and data protection, backup and disaster recovery testing, and IoT enablement with proper isolation. We keep today stable while preparing for tomorrow.

Support

Help desk surge capacity, staff augmentation, training, and organizational change management. Your people spend more time on strategy and less time chasing tickets.

Scope clarity

Co-managed means partnership. We do not replace your team. We define handoffs, set service levels, and bring in the right SMEs to run networks, augment staff, or provide vCISO advisory without overstating roles.

Our time-tested approach

Leaders want a path they can see and measure. MGT evaluates people, process, and technology, then delivers results through six practical phases. The outcome is a road map that reduces risk and clarifies priorities.

01 Discovery

We request artifacts such as policies, diagrams, inventories, and monitoring baselines. Evidence is collected once, then reused in later phases.decisions.

02 Workshops

We align scope and goals with the right stakeholders, confirm handoffs, and define service levels.

03 Evaluation

We score policy and practice quantitatively. This reveals gaps that can be closed quickly and gaps that require projects.

04 Refinement

We reconcile artifacts, close near-term gaps, and tune processes so daily work creates the evidence you will need later.

05 Recommendations

We present a phased, budget-aligned road map with clear owners and timelines.

06 Exercises and Validation

White-box penetration testing and tabletop exercises confirm that controls work in practice, surface gaps safely, and generate evidence you can show to auditors and boards.

M-powered

Unleash your team to be the strategists you hired them for

No network is perfect. It takes constant maintenance and continuous improvement.

We help you understand what skills you need in-house and what tasks to outsource.

With MGT, your team gets back to being strategic thinkers instead of getting stuck in day-to-day firefighting. Co-managed coverage also makes recruiting easier because your internal roles stay focused and attractive.

Why break-and-fix fails airports

Reactive repair looks inexpensive until you count disruption, overtime, reputational risk, and stalled modernization. The issue is rarely policy. It is execution at two in the morning. **A co-managed operating model makes prevention routine and provable** with measurable SLAs and a burn-down of technical debt month by month.

M-powered

MGT airport success stories

Houston Airport System

Project

MGT is in Year 2 of a potential 5-Year Managed Services Agreement to deliver managed public Wi-Fi at George Bush Intercontinental (IAH) and William P. Hobby (HOU) airports. Services include full NOC support and local onsite support. The technology supported includes Aruba Access Points, Controllers, Beacons for wayfinding/blue-dot location, ClearPass, and Palo Alto Firewalls. Additional wireless infrastructure upgrades are underway along with a wireless survey and assessment of both airports.

Outcome

Seamless, secure, and high-performance Wi-Fi for millions of travelers, supporting the Airport Passenger App with real-time wayfinding and enabling Houston Airports to scale and future-proof their digital infrastructure to meet growing passenger demands.

Rhode Island Airport Corporation (RIAC)

Project

RIAC engaged MGT to redesign their aging infrastructure and security practices to meet NIST standards and TSA regulations. Since 2020, MGT has delivered multiple projects across network, security, systems, and identity access management.

Outcome

MGT audited RIAC's entire IT environment, identified and remediated gaps, built an incident response plan with a table-top exercise, developed IT security policies in line with federal standards, and implemented vulnerability management services. An IT road map was also created to guide future progress.

Impact

RIAC emerged as a more reliable and trusted transportation services provider. IT outages improved from one per month to less than one per year through MGT's cost-effective solutions, policies, and operations.

ORCA – Sound Transit, Seattle, WA

Project

MGT first provided on-call incident response for the new regional fare system application and now delivers multi-year managed 24/7 detection and response along with incident response support.

Outcome

MGT delivers always-on monitoring and rapid response capabilities that safeguard ORCA's fare system and ensure continuity for riders across the Puget Sound region.

Client Testimonial

"MGT took the time to understand our needs and even worked with me after hours to find the best long-term solution for us. From the start MGT emphasized a desire to not just be a vendor but instead a partner in it for the long haul dedicated to impact.

Ashley Bowman
Business Manager, Regional Fare Systems

M-powered

Stronger IT leads to stronger airport operations

When back-of-house technology is disciplined and provable, the airport runs better:

- **Reliable access to critical systems for staff, tenants, and operations, plus resilient guest Wi-Fi that supports the customer journey.**
- **Stronger digital safety with identity, segmentation, and tested incident response.**
- **More time for strategic work, because your team is not chasing tickets.**
- **Confidence with partners and boards through evidence-ready reports and road maps.**
- **Fewer disruptions and faster fixes through proactive monitoring and clear escalation.**

Quick self-assessment: Is co-managed IT right for your airport

Answer Yes, No, or Not Sure to each of the questions:

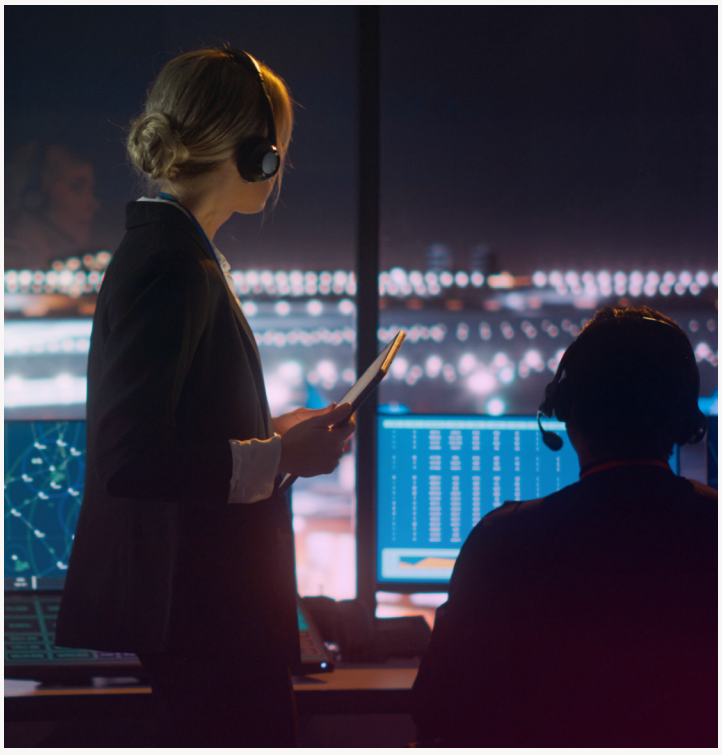
01 **Spending Balance**
Does your airport invest more in the front-of-house projects than in back-of-house network security, modernization and resilience?

02 **Modernization Gap**
Are your critical IT systems overdue for a refresh or segmentation?

03 **Compliance Confidence**
Can you prove alignment with TSA's 2023 cybersecurity requirements and 49 CFR Part 1542 today?

04 **People and Focus**
Does your IT staff act as strategic leaders (or are they stuck in daily firefighting)?

05 **Response Readiness**
If a breach hit at 2 a.m. tomorrow morning, could your team execute a tested incident response plan with named roles and current contacts?



If you answered **No** or **Not Sure** to any of these questions, your airport may benefit from a strategic readiness review by MGT.

We can help identify your risk gaps, deliver quick wins, and produce a phased road map that strengthens safety, compliance, and uptime for the long term.

M-powered

FAQs: What to expect with co-managed IT

Does co-managed IT replace our internal team?

No. It supports and strengthens your team. You stay in control while gaining extra hands, deeper expertise, and continuous coverage when and where you need it.

How fast can we get started?

Most airports see measurable impact within the first month. Our onboarding plan is designed to be phased with low disruption to daily operations.

Can you help with OT and third-party risk?

Yes. We segment and monitor OT networks, validate controls with penetration tests and tabletop exercises, and harden vendor handoffs.

Will we lose control of systems or decisions?

No. You will continue to own IT strategy, decisions and approvals. We help you execute, measure, and improve.

What about regulatory audits?

Our co-managed operations generate the logs, reports, and drill results that become your evidence packs for TSA's 2023 requirements and for 49 CFR Part 1542 obligations.

Be M-powered with MGT Managed Solutions

MGT is built to meet the evolving IT demands of airports. We support cybersecurity, network infrastructure, cloud and data, and communications. **Our model is co-managed by design, so your team stays in control while extending its reach.**

Whether you want to reduce costs, simplify operations, or strengthen resilience, MGT can help you be M-powered. Let us align on your goals, run a readiness checklist, and deliver a phased road map that strengthens your airport's network and cybersecurity.

References

- TSA press release. New cybersecurity requirements for airport and aircraft operators. March 7, 2023. TSA
- eCFR. 49 CFR Part 1542, Airport Security Program. Subparts A to D. eCFR
- Federal Register and FAA program pages. Safety Management Systems for Part 139 airports, final rule and implementation resources. Federal Register+1
- Port of Seattle. Notice regarding the August 2024 cyberattack, with approximately 90,000 people affected. Port Seattle
- The Record. Port of Seattle says 90,000 impacted in 2024 ransomware attack. April 4, 2025. The Record from Recorded Future
- Reuters and AP. European airport disruptions linked to third-party ransomware, September 2025. Reuters+1
- U.S. Census Bureau America Counts. Who Manages the Nation's Airports. 435 independent airport authorities and commissions. Dec 10, 2024. Census.gov