

Why Hospitality Organizations Choose AdvancedBITS: A Buyer's Guide to Choosing a Managed IT and Cybersecurity Partner

Why hotels and management companies choose AdvancedBITS, how to tell whether managed IT fits, and what to ask any provider before you sign

About this guide

This is a buyer's guide, not a client case study. It describes no client outcomes and carries no survey statistics. Where it cites guidance, the source is a government agency, a standards body, or a public record, and current statistics appear on our hospitality technology and AI page. Every statement about AdvancedBITS is written so that you can check it yourself.

Executive takeaway

A hotel runs on technology that cannot stop: reservations, check-in, payments, room access, Wi-Fi, and the email that holds owners, brands, vendors, and guests together. Your IT provider holds the keys to all of it, around the clock, across every property.

Hospitality organizations choose AdvancedBITS because we treat that technology as guest-facing infrastructure. We work in guest-impact order, handle payment security and vendor access together, prove recovery instead of promising it, and fit a single property or a whole portfolio. Table 1 shows what that means in practice and how you can verify each point. The rest of this guide helps you compare any provider, including us.

Many hospitality companies choose an IT provider the way they choose any other vendor: by price, by a brand recommendation, or by who answers first. That works until the front desk cannot check guests in, a vendor's remote-access tool becomes the way in, or an owner asks for evidence nobody kept. A few hours of structured questions before you sign cost far less than changing providers in the middle of a season.

Why hospitality organizations choose AdvancedBITS

AdvancedBITS helps hospitality organizations improve guest experiences, reduce risk, and strengthen operations through smarter technology, with enterprise-level expertise and without enterprise-level complexity. We act as an extension of your team, whether you have property IT staff we support or no IT staff at all. Table 1 gives six reasons, what each means for a hotel operation, and how to check it. We encourage you to check, because the rest of this guide shows you how.

Table 1. Six reasons hospitality organizations choose AdvancedBITS

Reason	What it means for a hotel operation	How to verify it
1. We treat IT as guest-facing infrastructure	We set recovery priorities in guest-impact order: reservations and check-in, payments, room access, Wi-Fi, email, then back office. We stage changes around occupancy peaks, and we agree front-desk downtime procedures with property leaders before we touch front-desk systems.	Ask to see a sample recovery-priority list and a downtime procedure.
2. Security aimed at what guests touch	Sign-in protection with individual front-desk accounts, second-channel verification before any password or MFA reset, email and booking-themed phishing defense, endpoint protection and patching, and guest Wi-Fi kept apart from payment and operational systems.	Ask for the control list and a sample evidence report.
3. Payment security and vendor access, handled together	PCI DSS security support: we map technical responsibilities across your systems, vendors, and teams, document payment flows, and build one inventory of PMS, POS, Wi-Fi, keycard, and camera vendors, with time-limited, logged remote access. Your acquirer or qualified assessor decides scope, and the vendors remain responsible for their own systems.	Ask for our responsibility matrix and a sample vendor inventory.
4. Proof, not promises	We test restores, keep dated evidence, and give owners, brands, and insurers a regular report on security, recovery, assets, and the roadmap. Our security practice is examined by an independent CPA firm under SOC 2 Type II.	Ask for a sample report and ask to read the SOC 2 report.
5. A model that fits a portfolio	Co-managed or fully managed, with a common baseline for devices, accounts, onboarding, and support across properties, so a new hotel joins a standard instead of a one-off. We work within brand technology standards.	Ask how a new property is onboarded and what is standard.
6. AI with guardrails	We find out what teams already use, clean up Microsoft 365 permissions, set simple rules, require human review of anything a guest sees, and pilot low-risk uses first.	See our AI in Hospitality case study.

What we can substantiate

Table 2. What AdvancedBITS can show you

What we say	What it means for you	How to verify it
More than 11 years of managed services experience, and incorporated in 2015	A track record, not a first attempt.	Ask for references from clients who have been with us the longest.
98% client retention. The clients we have lost left because they were acquired by a larger firm or closed their business.	Clients tend to stay.	Ask references how long they have been with us and what keeps them here.
A SOC 2 Type II examined security practice	An independent CPA firm has examined our controls over a period of time.	Ask to read the opinion, the period covered, and any exceptions.

What we say	What it means for you	How to verify it
Clients across manufacturing, legal, insurance, finance, private equity, M&A, services, property management, and hotel management	Experience protecting confidential data and working with clients who answer to owners, regulators, insurers, and customers.	Ask for references from organizations like yours.

When we may not be the right fit

- If you operate a single small property whose brand manages the core systems and you need occasional help with a few devices, a break-fix technician may cost less.
- If you need a formal PCI DSS assessment or attestation, that comes from a qualified assessor, and we work alongside them.
- If you need legal, tax, accounting, or insurance judgement, we work alongside your attorney, accountant, and broker, and we do not replace them.

Is it time for managed IT?

You do not need an incident to justify outside help. Most hospitality organizations move to managed IT when several small signs have added up. Table 3 lists the common ones and the first step for each.

Table 3. Signs that managed IT may fit, and what to do first

Sign	What it usually means	First step
One person covers technology for several properties	A single point of failure, especially during peak periods and vacations.	Document what they know, and add coverage behind them.
Every property is set up a little differently	Inconsistent standards, uneven security, and slow onboarding of new properties.	Create a common baseline for devices, accounts, and support.
Vendors have remote access nobody tracks	PMS, POS, Wi-Fi, keycard, and camera vendors may have standing access to your network.	List every vendor, what it can reach, and who owns the relationship.
Front-desk sign-ins are shared	Accountability gaps, and access that never ends when staff leave.	Move to individual accounts and a clean joiner, mover, and leaver process.
Nobody can say when a recovery was last tested	Recovery is assumed, not proven, for the systems guests depend on.	Run and time a restore of real data.
Owners, brands, lenders, or insurers ask for security evidence	You need controls you can show, with dates.	Inventory your controls and keep dated evidence.
Staff use AI tools nobody approved	A governance gap around guest and company data.	Ask what people use, then write simple rules.

Managed IT is not for everyone. A single small property whose brand already manages its core systems, with an owner who keeps sign-in protection and backups current, may not need a full program. Many franchised hotels also operate under brand technology standards, so any provider you hire should work within them. A short assessment can confirm which situation you are in.

Three ways to get IT support

The difference between models is who owns what. Break-fix means you call a technician when something breaks. Co-managed IT adds a provider alongside your own IT person or team, covering the gaps. Fully managed IT makes the provider your IT department. Table 4 shows the typical split for a multi-property organization. Your contract should state yours, because the joint advisory on managed service providers from CISA and its international partners advises that contracts transparently identify who owns security roles and responsibilities.

Table 4. Who does what in each support model

Responsibility	Break-fix	Co-managed	Fully managed
Property and corporate help desk	You call a technician when something breaks	Your team handles daily requests, and the provider handles overflow, nights, and escalations	The provider
Security monitoring and patching	Usually no one, unless you ask	The provider	The provider
Backup and restore testing	Your responsibility	The provider, with your input on recovery priorities	The provider
Microsoft 365 administration	Ad hoc	Shared by agreement	The provider
Network and guest Wi-Fi	Quoted when it breaks	Shared, with the provider owning standards and monitoring	The provider
PMS, POS, and other vendor coordination	You	Shared, with a single owner named for each vendor	The provider coordinates, and the vendor remains responsible for its own system
PCI DSS security support	Your responsibility	Responsibilities split in writing	Responsibilities split in writing
Reporting to ownership and brands	None	Your lead owns it, with provider support	The provider, reviewed with leadership

These are typical splits, not guarantees. Ask any provider to show you the responsibility split in writing, property by property if your portfolio varies.

Which fits? If you have no internal IT, or you want technology off your plate, fully managed is the cleaner fit. If you have an IT person or team you value who is stretched across properties, co-managed keeps their knowledge and adds depth around it, including overnight coverage. A short break-fix arrangement can work for a very small, low-risk property. AdvancedBITS provides both co-managed and fully managed IT.

How to evaluate any provider, including us

Compare providers on evidence, not on how confident they sound. Three points deserve explanation before the checklist.

The provider's own access is part of your perimeter. The joint advisory from CISA, the FBI, the NSA, and the cyber agencies of the United Kingdom, Canada, Australia, and New Zealand

advises managed service providers and their customers to enforce multi-factor authentication on provider accounts that access customer environments, to disable accounts no longer in use, and to state security roles in the contract. Public reporting on the 2023 cyberattack on MGM Resorts, summarized on our hospitality technology and AI page, describes an intrusion that began with a social-engineering call to the IT help desk. Whether a provider verifies a caller before resetting a password or a multi-factor device is therefore a real control, and worth asking about.

Payment security reaches your IT provider. The Payment Card Industry Data Security Standard (PCI DSS) is a contractual standard maintained by the PCI Security Standards Council and enforced through card-brand rules and acquirer agreements. Version 4.0.1 is the current version, and its requirements introduced as future-dated became mandatory on March 31, 2025. Under Requirement 12.8, an organization must manage the third-party service providers that handle account data or can affect the security of its cardholder data environment, which typically includes managed IT and security vendors with access to that environment. That means keeping a list of those providers, holding a written agreement that records each provider's responsibilities, performing due diligence before engaging them, and monitoring their compliance status each year. Requirement 12.9 asks those providers to acknowledge their responsibility in writing. Your acquirer or qualified assessor decides how this applies to you, and a provider should be able to tell you in writing which requirements it supports.

Network separation helps, but it has to be real. The PCI Security Standards Council advises starting from the assumption that everything is in scope until verified otherwise. It notes that segmentation can reduce the number of systems in scope, but that it is not a silver bullet, and that attackers often target systems an organization has deemed out of scope. Ask any provider how separation is designed, tested, and maintained.

Table 5. What to check, and what the answers tell you

Area	What good looks like	How to check	A warning sign
1. The provider's own access	MFA enforced on every provider account that reaches your systems. Individual accounts, logged access, and removal when staff leave.	Ask how technicians sign in to your environment.	A shared administrator login.
2. Help desk verification	A documented second-channel check before any password or MFA reset, with extra steps for administrators and executives.	Ask them to walk you through a reset request from an unknown number.	"We recognize our clients' voices."
3. Independent assurance	A current SOC 2 Type II report or a similar independent examination.	Ask to read the opinion, the period covered, and any exceptions.	"We follow best practices," with nothing to read.
4. PCI DSS responsibilities	A written responsibility matrix showing what the provider, your vendors, and you each own, and the provider's willingness to acknowledge its part.	Ask for the matrix and confirm scope with your acquirer or assessor.	"You'll be fine," with no document.
5. Hospitality platforms and brand standards	Familiarity with PMS, POS, reservation, keycard, and Wi-Fi vendors, and respect for brand technology standards.	Ask which platforms they support today and how they work with the vendor.	A plan to replace what the brand requires.

Area	What good looks like	How to check	A warning sign
6. Vendor remote access	An inventory, time-limited and logged access, MFA, and a named owner for each vendor.	Ask to see a sample inventory.	Standing access that nobody reviews.
7. Network separation	Guest Wi-Fi, payment systems, operational systems, IoT, and management networks are separated, with documented rules and scheduled tests.	Ask to see the network design and the last test.	"It's all one network, but we have a firewall."
8. Always-on support and recovery	Response targets by severity, after-hours coverage, written front-desk downtime procedures, and dated restore tests.	Ask what happens at 2 AM on a holiday weekend and ask for the last restore result.	"Open a ticket and we will get to it."
9. Reporting	A regular report for owners, brands, and insurers covering security, recovery, assets, and the roadmap.	Ask for a sample report.	"Call us any time," and nothing in writing.
10. Scope, exit, and references	Transparent fees, documentation you own, an orderly handover if you leave, and references from clients like you.	Read the contract and ask for a current client and a former client.	Fees or friction to retrieve your own information.

On SOC 2 specifically: the AICPA describes SOC 2 as a report on an examination of a service organization's controls. A Type II report covers how those controls operated over a period of time, and it is an attestation by an independent CPA firm rather than a certificate. That is why the right request is to read the report, not just to ask whether a provider has one.

Contract terms to read twice

The contract tells you what the relationship will be like when something goes wrong.

Table 6 lists the terms worth a second read for a hospitality portfolio. Contracts vary, so have your attorney review before you sign.

Table 6. Contract terms to check

Term	What to check	Why it matters
Scope by property	Which properties, users, devices, and systems are covered, how new properties are added, and what counts as a separate project.	Portfolios change, and billing surprises come from assumptions.
Security and PCI responsibilities	Who owns identity, endpoints, network, backup, incident response, and each PCI DSS requirement the provider supports.	Government and payment-industry guidance both call for roles to be written down.
Response commitments	Targets by severity, with front-desk, payment, and reservation outages treated as critical.	"Fast" is not a commitment.
Incident communication	Who tells whom, and how quickly, including owners, the brand, your acquirer, and your insurer.	Confusion in the first hours is expensive.
Seasonal and brand changes	How the provider handles seasonal staff, new openings, rebrands, and brand technology standards.	Hospitality changes shape with the season.
Term and renewal	Length, automatic renewal, and the notice you must give.	Long terms with no exit clause reduce your leverage.

Term	What to check	Why it matters
Termination and handover	What you receive on exit, in what format, and at what cost.	You should be able to leave with your documentation.
Data and documentation ownership	Who owns configurations, network diagrams, credentials, and records.	The environment is yours, and so is the knowledge of it.

How an engagement with AdvancedBITS starts

You can judge us before you commit. The first steps are designed so you see how we work while the stakes are low. Table 7 shows the path, and Table 8 shows what the first 100 days usually cover.

Table 7. How an engagement starts

Step	What happens	What you receive
1. A conversation	We learn what you depend on, what slows your properties down, and what worries you.	A shared picture of the goal.
2. A complimentary assessment	We review sign-in protection, Microsoft 365, networks, vendor access, backup and recovery, AI use, and key vendors.	A plain-language list of priorities, with no obligation.
3. A written plan	We turn the priorities into a plan with owners, sequence, and budget ranges.	A roadmap you can approve, change, or take elsewhere.
4. Onboarding and the first 100 days	We close the highest risks, document the environment, and test recovery.	Controls in place and evidence on file.
5. Ongoing management and review	We provide support, monitoring, and patching, and review results with you regularly.	Steady operations and a view of what is next.

Table 8. The first 100 days

Timeframe	Priorities	Done when
Days 1 to 30: See	Inventory users, devices, Microsoft 365 settings, PMS, POS, and other platforms, vendors and their access, networks, backups, security tools, AI use, and critical workflows.	Leadership can name what the business depends on, where the gaps are, and who owns each one.
Days 31 to 60: Secure	Close MFA and endpoint gaps, strengthen email security, separate networks, review vendor access, set up backup, fix Microsoft 365 permissions, and adopt AI rules.	Common risks are closed, vendor access is controlled, and the AI rules are written and shared.
Days 61 to 100: Prove and plan	Test a restore, write front-desk downtime procedures, run a leadership tabletop exercise, pilot low-risk AI uses, and build a budgeted roadmap.	A timed restore is on file, and leadership has approved a roadmap.

Related resources

- For managed IT, cybersecurity, Microsoft 365, and the independent research, see our [hospitality technology and AI page](#).

- For a worked security and continuity scenario, see our Cybersecurity in Hospitality case study.
- For a worked AI adoption scenario, see our AI in Hospitality case study.

Frequently asked questions

Why should a hotel management company choose AdvancedBITS?

Because we treat your technology as guest-facing infrastructure: we work in guest-impact order, handle payment security and vendor access together, prove recovery with restore tests and dated evidence, and fit a single property or a whole portfolio. Table 1 lists six reasons and how to verify each one, and we encourage you to compare us with any other provider using Table 5.

Is managed IT worth it for a hotel management company?

It is worth it when the cost of downtime, a security incident, or a stretched employee exceeds the cost of structured support. Look at how much each property depends on technology, who owns it today, and whether you can show that backups, vendor access, and security controls work. A short assessment can answer it for your situation.

What is the difference between co-managed and fully managed IT?

In co-managed IT, a provider works alongside your own IT person or team and covers gaps such as overnight monitoring, security, and projects. In fully managed IT, the provider acts as your IT department. Table 4 shows the typical split. AdvancedBITS provides both.

Does my IT provider need to be PCI compliant?

PCI DSS asks you to manage third-party service providers that handle account data or can affect the security of your cardholder data environment, which typically includes managed IT and security vendors with access to it. Ask any provider which requirements it supports and to put that in writing. Your acquirer or qualified assessor decides how the standard applies to you.

What should I ask an IT provider before signing?

Ask how their technicians access your systems, how they verify callers before resets, whether you can read their independent security report, which PCI DSS requirements they support, what happens during a front-desk outage at night, when they last restored a client's data, and what you receive if you leave. Table 5 lists ten areas with the answers to listen for.

What does SOC 2 Type II mean for my IT provider?

It means an independent CPA firm examined the provider's controls and reported on how they operated over a period of time. It is a report, not a certificate, so ask to read the opinion, the period covered, and any exceptions.

Will changes disrupt our operation?

They should not. Start with a read-only assessment, stage changes around occupancy peaks, agree front-desk downtime procedures before touching those systems, and tell property teams what is changing and when.

What happens to our documentation if we leave?

It should be yours. Ask every provider, including us, to state in writing what you receive on exit, in what format, and at what cost.

Take the next step

Schedule your complimentary Hospitality Technology & Risk Assessment. We will review your sign-in protection, Microsoft 365, networks, vendor access, backup and recovery, and AI use, then give you plain-language priorities, with no obligation. Call **561-300-3015** or email sales@advancedbits.com.

AdvancedBITS | Business IT Solutions | www.advancedbits.com

Sources

References were opened and checked as of October 22, 2026. The PCI DSS explanations come from the PCI Security Standards Council, a QSA-reviewed guide, and a compliance vendor, so confirm how the standard applies to you with your acquirer or qualified assessor. Co-managed and fully managed definitions reflect common industry usage, as described by providers.

1. Cybersecurity and Infrastructure Security Agency, with the FBI, NSA, and the cyber agencies of the United Kingdom, Canada, Australia, and New Zealand. Protecting Against Cyber Threats to Managed Service Providers and their Customers, Advisory AA22-131A (May 11, 2022). <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a>
2. AICPA and CIMA. Illustrative SOC 2 Report with Illustrative System Description (September 30, 2023). <https://www.aicpa-cima.com/resources/download/illustrative-soc-2-r-report-with-description-and-assertion>
3. SOC2Auditors.org. SOC 2 Type 2 Report: What It Is, What's Inside, How to Read, on the report as an attestation rather than a certification. <https://soc2auditors.org/insights/what-is-a-soc-2-type-2-report/>
4. PCI Security Standards Council. Document Library, including PCI DSS v4.0.1 (June 2024). https://www.pcisecuritystandards.org/document_library/
5. PCI Security Standards Council. Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation (December 2016), source of the scoping assumption and the limits of segmentation. https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf
6. PCIDSSGuide.com. PCI DSS Third-Party Service Provider Management (v4.0.1), updated September 2026. <https://pcidssguide.com/what-are-the-pci-dss-third-party-service-provider-management-requirements/>
7. Rescana. PCI DSS and third-party risk: managing TPSPs under Requirement 12.8 (updated September 10, 2026), source of the March 31, 2025 effective date. <https://www.rescana.com/learn/compliance/pci-dss-third-party-risk/>
8. Toulas, B. BleepingComputer. MGM Resorts ransomware attack led to \$100 million loss, data theft (October 6, 2023), on the social-engineering entry point. <https://www.bleepingcomputer.com/news/security/mgm-resorts-ransomware-attack-led-to-100-million-loss-data-theft/>
9. Specops Software. MGM Resorts hack: How attackers hit the jackpot with service desk social engineering (updated November 12, 2025), vendor analysis of public reporting on how the intrusion began. <https://specopssoft.com/blog/mgm-resorts-service-desk-hack/>
10. Allen IT. Co-Managed Versus Fully Managed IT Compared (August 31, 2026). <https://allenit.net/co-managed-versus-fully-managed-it/>
11. Balanced+. How Are Co-Managed IT and Fully Managed IT Different? (June 30, 2026). <https://balanced.plus/how-are-co-managed-it-and-fully-managed-it-different/>