BTI COMMUNICATIONS GROUP
2027 EDITION · PROOF v1
Last reviewed: October 2026
Next review: January 2027

FOR CEOS, COOS, CFOS AND IT LEADERS AT REGULATED AND MULTI-SITE ORGANIZATIONS

The Executive Guide to Managed IT and Cybersecurity

How to tell when you have outgrown your IT model, what a unified IT, security and network operation looks like, the 2026-2027 deadlines to plan for, and how to evaluate a provider.

A concise executive briefing with a signs-you've-outgrown checklist, an operating-model comparison, a dated compliance calendar, AI-readiness guidance and a fillable provider scorecard.

INSIDE THIS GUIDE

- Signs you have outgrown your current IT or MSP model
- Fully managed vs. co-managed vs. in-house: when each fits
- 2026-2027 calendar: Windows 10 ESU, CMMC, HIPAA, PCI DSS, Reg S-P
- AI readiness and governance for leadership teams
- Fillable 10-point provider scorecard

Talk to a BTI business advisor

Request an IT and security operations readiness review for your organization.

National
800-435-7284
info@btigroup.com

LOS ANGELES 323-510-8002 **CHICAGOLAND** 312-432-5300 **PHOENIX** 602-733-6807
www.btigroup.com/contact · www.btigroup.com/it-services/managed-it/

Serving businesses since 1985 · Integrated security since the 2010s · ISO 27001 compliant · GSA, CMAS & TESMA contracts · ACO licensed in CA, AZ & IL

At a glance

SHORT ANSWER

Managed IT and cybersecurity means an outside provider runs some or all of your IT operations (help desk, devices, network, cloud) and security operations (monitoring, detection, response, evidence) under defined service levels. Growing, regulated and multi-site organizations usually outgrow a patchwork of vendors when outages, audit requests and security incidents start falling between them. A unified model, either fully managed or co-managed with your internal team, gives one accountable owner across IT, cybersecurity, network and communications.

$10.22M
Average cost of a US data breach (global $4.44M)
IBM Cost of a Data Breach 2025[1]

$122
Per-device price of Windows 10 commercial ESU Year 2, starting Oct 14, 2026
Microsoft[2]

July 2027
Projected final action on the HIPAA Security Rule update
reginfo.gov[4]

Contents

Signs you have outgrown your IT model 3
Choosing an operating model 4
2026-2027 compliance and risk calendar 5
Provider scorecard (fillable) 6
Frequently asked questions 8
Sources and change log 9

Signs you have outgrown your IT model

- ☐ Outages or security issues bounce between vendors (ISP, MSP, phone, security-system installer) with no single owner
- ☐ Audit, customer or cyber-insurance questionnaires take weeks and rely on one person's memory
- ☐ Your internal IT team spends most of its time on tickets instead of projects
- ☐ New sites take months to open because network, Wi-Fi, phones and security systems are separate projects
- ☐ There is no current asset inventory, network diagram or tested incident-response plan
- ☐ Leadership cannot see IT and security risk in a quarterly report
- ☐ AI tools are in use with no approved list or data rules

Choosing an operating model

	In-house only	Co-managed	Fully managed
Who does the work	Your staff	Your team plus provider for defined functions	Provider, with your leadership oversight
Best for	Large IT teams with security depth	Organizations with an IT lead or small team	Organizations without dedicated IT staff
24x7 coverage	Hard to staff	Provider covers after-hours and security monitoring	Included
Typical split	n/a	You: strategy, apps, users; provider: monitoring, SOC, projects, overflow	Provider: help desk, devices, network, security; you: approvals and budget

Unified operations: the industry is moving toward one operational view across network, security and IT; Cisco's Cloud Control (announced June 2, 2026), for example, brings Cisco domains under one login with AI agents that work under human control.[6] Whatever the tools, insist on one accountable owner and shared documentation.

Talk to a BTI business advisor about your managed IT and security operations

A BTI business advisor will review your sites, current systems and requirements, then outline options, timelines and budget ranges. No obligation.

Contact a BTI business advisor | Managed IT services

Call 800-435-7284 (national) · Los Angeles 323-510-8002 · Chicagoland 312-432-5300 · Phoenix 602-733-6807 · info@btigroup.com

2026-2027 compliance and risk calendar

Date	Item	Action
Mar 31, 2025	PCI DSS v4.0.1 future-dated requirements mandatory[5]	Confirm scope, MFA and logging for cardholder systems
June 3, 2026	SEC Reg S-P amendments apply to smaller covered institutions[7]	Incident-response program and 30-day customer notice
July 13, 2026	DoD memo suspends CMMC Phase 2; L1/L2 self-assessments continue; DFARS 7012 still applies[3]	Keep NIST SP 800-171 work moving
Oct 14, 2026	Windows 10 ESU Year 2 ($122 per device; late enrollment also requires Year 1)[2]	Replace or enroll remaining Windows 10 devices
July 2027	Projected final HIPAA Security Rule update; current rule enforceable[4]	Plan for MFA, encryption, asset inventory and segmentation

AI readiness for leadership teams

- **Policy first:** approved AI tools, what data may be entered, and who approves new uses.
- **Identity and data hygiene:** AI tools surface whatever users can access; clean up permissions before broad rollout.
- **Agents with guardrails:** least privilege, human approval for changes, logged actions.
- **Measure value:** pick two or three workflows, set baselines and review after 90 days.

BTI's AI services team can help assess readiness and governance: AI services and solutions.

Provider scorecard (fillable)

Rate each provider you are evaluating: **Strong = 2, Partial = 1, Missing = 0** (maximum 20).

#	Criterion	Strong	Partial	Missing
1	Single accountable owner for IT, cybersecurity, network and communications issues	◯	◯	◯
2	24x7 monitoring with defined response and resolution times in the contract	◯	◯	◯
3	Security operations included (endpoint detection, log monitoring, incident response), not an add-on surprise	◯	◯	◯
4	Documented onboarding: asset inventory, credentials vault, network diagrams within 30-60 days	◯	◯	◯
5	Evidence packages for audits, customers and cyber insurance on request	◯	◯	◯
6	Co-managed option that works alongside your internal IT team	◯	◯	◯
7	On-site capability in your regions (cabling, Wi-Fi, security systems) without subcontractor hand-offs	◯	◯	◯
8	Quarterly business reviews with metrics and a lifecycle budget	◯	◯	◯
9	Clear exit terms: documentation and credentials returned on termination	◯	◯	◯
10	AI governance support: approved tools, data rules and agent guardrails	◯	◯	◯

Provider: _____ Score: _____ / 20

How BTI helps

BTI has served businesses since 1985 and delivers managed and co-managed IT, cybersecurity, network and Wi-Fi, communications and integrated security systems from offices in Los Angeles, Chicagoland and Phoenix. BTI is ISO 27001 compliant.

Engagement	What it includes
Readiness review	Current-state inventory, risk and evidence gaps, roadmap
Co-managed IT	Monitoring, security operations, projects and overflow alongside your team
Fully managed IT	Help desk, devices, network, cloud and security operations
Projects	Network, Wi-Fi, SD-WAN, security systems and site openings

Related BTI pages: Managed IT · Managed IT pricing · Co-managed IT · Help desk · Cybersecurity · Infrastructure-led managed IT

About BTI Communications Group

BTI Communications Group (BTI Group) has served businesses since 1985 (40 years) and has delivered integrated security systems since the 2010s, alongside managed IT, cybersecurity services, networking and business communications. BTI focuses on high-security, regulated and multi-site organizations in healthcare, financial services, logistics, manufacturing, education and the public sector.

Credential	Detail
Security management	ISO 27001 compliant information security practices
Public-sector contracts	GSA, CMAS and TESMA contract vehicles
Licensing	Alarm Company Operator (ACO) licenses in California, Arizona and Illinois
Offices	Los Angeles 323-510-8002 · Chicagoland 312-432-5300 · Phoenix 602-733-6807 · National 800-435-7284

Frequently asked questions

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

Managed IT hands day-to-day operations to the provider; co-managed IT splits responsibilities between your team and the provider, typically with the provider covering monitoring, security operations, after-hours and projects.

How do I know if I have outgrown my MSP?

Recurring finger-pointing between vendors, slow audit responses, no current documentation and no security reporting to leadership are common signs.

What should a managed security service include?

24x7 monitoring, endpoint detection and response, log review, an incident-response process, vulnerability management and evidence for audits and insurers.

What happens to Windows 10 PCs now?

Microsoft's commercial ESU Year 2 runs Oct 14, 2026 to Oct 12, 2027 at $122 per device; replacing devices is often the better investment.[2]

Does BTI publish managed IT pricing?

BTI publishes pricing guidance on its managed IT pricing page; a business advisor can scope your environment.

Ready to scope your managed IT and security operations?

A BTI business advisor will review your sites, current systems and requirements, then outline options, timelines and budget ranges. No obligation.

Contact a BTI business advisor **Managed IT services**

Call **800-435-7284** (national) · Los Angeles **323-510-8002** · Chicagoland **312-432-5300** · Phoenix **602-733-6807** · **info@btigroup.com**

Sources and change log

1. IBM, "Cost of a Data Breach Report 2025" and IBM Newsroom, July 30, 2025. https://www.ibm.com/reports/data-breach
2. Microsoft Learn, "Extended Security Updates for Windows 10." https://learn.microsoft.com/windows/whats-new/extended-security-updates
3. DoD CIO, "Implementing Suspension of CMMC Phase II," memo dated July 13, 2026. https://dodcio.defense.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf
4. Unified Agenda, RIN 0945-AA22 (HIPAA Security Rule NPRM; final action 07/2027). https://www.reginfo.gov/public/do/eAgendaViewRule?RIN=0945-AA22&pubId=202510
5. PCI Security Standards Council, PCI DSS v4.x. https://www.pcisecuritystandards.org/standards/pci-dss/
6. Cisco Newsroom, "Cisco Unveils Agentic Platform for Operating and Defending Critical IT Infrastructure," June 2, 2026. https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2026/m06/cisco-unveils-agentic-platform-for-operating-and-defending-critical-it-infrastructure.html
7. SEC, "Regulation S-P" amendments. https://www.sec.gov/rules-regulations/2024/06/s7-05-23

Change log. 2027 edition proof v1 (Oct 11, 2026): condensed from 41 pages into an executive briefing. Added outgrown-checklist, operating-model table, dated compliance calendar, AI readiness and a fillable provider scorecard. Removed named cybersecurity and tooling partners, unsourced percentages and the "ISNetworld certified" line (pending confirmation).