2026 ENTERPRISE INFRASTRUCTURE FIELD GUIDE

The 2026 Enterprise Guide to Cisco & Cisco Meraki Infrastructure Modernization

HEALTHCARE · LOGISTICS · MANUFACTURING · FINANCIAL SERVICES · EDUCATION · GOVERNMENT

A practitioner's reference for IT directors, infrastructure architects, and operations leaders managing Cisco end-of-life transitions, Meraki wireless modernization, SD-WAN migration, and compliance-driven network refresh across enterprise and multi-site environments in 2026.

BTI Communications Group · Cisco Gold Partner · Cisco Meraki Partner

800-HELP-BTI · btigroup.com · Southern California · Phoenix · Chicagoland

TABLE OF CONTENTS

A practitioner's reference for infrastructure leaders navigating Cisco modernization, Meraki wireless, SD-WAN, and compliance-driven network refresh in 2026.

BTI Communications Group · Cisco Partner · Cisco Meraki Partner

800-HELP-BTI · btigroup.com · Southern California · Phoenix · Chicagoland

Executive Summary

In 2026, aging switching, legacy wireless, and fragmented security are active operational liabilities — not deferred maintenance. Cisco lifecycle transitions, cyber insurance requirements, and compliance-driven refresh cycles are forcing decisions that should have been made in 2024.

The Signs That Modernization Is Overdue

- **Cisco EoL hardware** — no patches, no TAC, active CVE exposure
- **Cyber insurance gap** — underwriters requiring documented segmentation
- **Wireless failures** — persistent complaints signal RF design, not hardware
- **AI initiative stalled** — edge compute requires purpose-built infrastructure
- **No vendor accountability** — reseller, integrator, MSP = no single owner
- **Outdated documentation** — diagrams older than 18 months are a liability

The Biggest Network Infrastructure Risks

- **Flat network** — one breach propagates across the entire environment
- **Undocumented topology** — cannot assess, insure, or migrate without it
- **No SD-WAN or WAN failover** — single circuit = single point of failure
- **Wireless dead zones** — operational failures in clinical and warehouse environments
- **Legacy firmware** — failures occur after deferred cycles, not planned refreshes

---

> **The infrastructure decision is already overdue. Every quarter of delay increases exposure, cost, and operational risk.**

Watch: How to do a Cisco Upgrade and Why Organizations Choose BTI to Help

This overview covers BTI's end-to-end approach to infrastructure modernization — from assessment through deployment and ongoing managed support.

ⓘ ▶️ **Watch on YouTube: Why Organizations Choose BTI for Cisco & Meraki Infrastructure**

BTI's infrastructure specialists walk through real-world deployment scenarios across healthcare, logistics, manufacturing, financial services, education, and government.

What You'll Learn

- BTI's full lifecycle delivery model in action
- How Cisco + Meraki architectures are designed for compliance
- Regional project capability across CA, AZ, and IL
- Real-world operational continuity outcomes

Who Should Watch

- IT Directors and CIOs evaluating Cisco refresh
- CISOs assessing cybersecurity infrastructure posture
- IT managers, operations directors, and procurement leaders comparing Cisco partner capabilities
- Warehouse managers, healthcare administrators, plant managers, school administrators, and municipal IT teams planning multi-site modernization

Why Infrastructure Decisions Can't Wait Until 2027

In 2026, aging Cisco infrastructure is a compliance liability, a cyber insurance risk, and a barrier to AI readiness.

5 Signs Your Infrastructure Is Overdue

- **Cisco switches past end-of-support (3850, 2960, ASA)**
- **Wireless complaints from staff or warehouse operators**
- **Cyber insurance requiring segmentation proof**
- **AI initiative blocked by network limitations**
- **No documented architecture or segmentation plan**

What's Driving the 2026 Refresh

- **Cisco end-of-life milestones forcing hardware decisions**
- **Zero Trust and segmentation mandates from insurers**
- **Wi-Fi 6/6E upgrades for high-density environments**
- **SD-WAN migration for multi-site cloud operations**

Why Cisco Infrastructure Projects Fail

Emergency-Driven Execution

Projects deployed under crisis conditions skip assessment, design, and validation phases.

Misestimated Requirements

Undersizing for current load or ignoring future density creates infrastructure obsolete at cutover.

Overengineered Out of Caution

Enterprise-grade complexity in environments requiring precision produces cost overruns and configuration debt.

Incompetent Configuration & Vulnerability Management

Misconfigured VLANs, default credentials, and unpatched firmware are the most common post-deployment failure sources.

> Measure twice, cut once — and contract with a provider who is responsible for both measuring and cutting.

Request an Infrastructure Risk Assessment → btigroup.com

How to Evaluate a Cisco Infrastructure Partner

The difference between a successful infrastructure modernization and a failed one comes down to four operational capabilities — not certifications.

4 Capabilities That Separate Accountable Partners from Resellers

Lifecycle Ownership

One partner owns design, deployment, documentation, and support. No handoffs.

Compliance Fluency

Demonstrated HIPAA, NIST, PCI-DSS, and CJIS experience — not claimed familiarity.

Regional Presence

Local project managers and on-site teams — not a remote national call center.

PMO Discipline

Formal governance, milestone tracking, and staged cutover planning.

Strong Partner Delivers

- Single accountable partner
- Audit-ready documentation
- Compliance-integrated architecture
- Staged migrations with rollback planning
- Ongoing managed services

Red Flags

- Hardware-only resellers
- No formal project management
- Remote-only support
- Documentation as afterthought
- No compliance framework experience

> The right Cisco partner owns the outcome — not just the hardware.

Evaluate BTI as your Cisco infrastructure partner → btigroup.com

Why Organizations Choose BTI

> **"Infrastructure modernization is not a product purchase — it is a program of work that requires a partner who owns the outcome and shares the risk of failure and scope creep." - Eric Brackett, Founder and President**

Converged Delivery

IT, cybersecurity, physical security, and VoIP under one accountable partner

Itemized Pricing and Guaranteed Deliverables

Detailed line item pricing at reduced cost plus fixed cost scopes save money.

Lifecycle Accountability

One team designs, installs, documents, and supports — no handoffs, no gaps

Regional Engineering

On-site engineers and PMs across Southern California, Phoenix, and Chicagoland

Continuity Ownership

Failover architecture, cutover windows, and post-deployment validation

---

How Clients Benefit From BTI

- IT, physical security, and VoIP expertise
- Compliance-integrated solutions
- Ekahau validated wi-fi heat mapping and on-site surveys
- Available discounted managed service

The Alternative

- Most integrators bill 1.5 times their estimates
- Many MSP's specify SMB gear at outsized markups.
- Client owns the risk of failure.
- Project fails to deliver Return on Investment

Start Your Infrastructure Modernization → btigroup.com

40 Years. Six Industries. One Methodology.

Cross-industry experience is an operational advantage — a segmentation architecture that protects clinical IoT in a hospital also protects OT systems on a factory floor.

Pattern Recognition Across Verticals

Solutions informed by real-world outcomes across healthcare, logistics, manufacturing, financial services, education, and government.

Compliance Fluency Built Over Decades

HIPAA, NIST, CIS, PCI-DSS, CJIS, E-Rate — navigated across hundreds of deployments.

Operational Continuity as a Core Discipline

Staged migration, PMO-governed cutover, and post-deployment validation protect operations at every phase.

Trusted Advisor Relationship

Many BTI clients started with a single upgrade — and grew into full lifecycle managed services.

40+

Years of Infrastructure Experience

6

Core Industry Verticals Served

3

Regional Markets: Southern CA · Phoenix · Chicagoland

> **"BTI's industry breadth means every new engagement is informed by hundreds of prior deployments — not a first attempt."**

Explore BTI's Infrastructure Capabilities → btigroup.com

Clinical Networks That Cannot Fail

Healthcare networks carry EHR, PACS imaging, clinical IoT, and AI diagnostics simultaneously — degraded performance is a patient care disruption.

Why Networks Fail

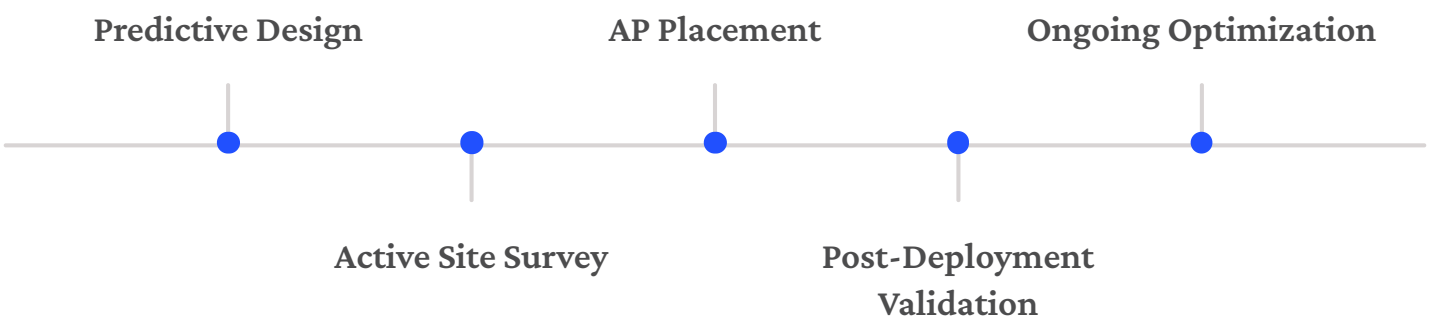
- PACS congestion during peak imaging hours
- EHR latency from poor QoS and VLAN design
- Nurse roaming failures from sticky client behavior
- RF interference from MRI and imaging equipment
- Flat networks with no medical IoT segmentation
- Undocumented topology failing HIPAA audits

What BTI Delivers

- Ekahau RF modeling and Wi-Fi 6/6E deployment
- Dedicated VLANs for medical IoT and nurse call
- HIPAA-aligned segmentation and access controls
- QoS engineered for peak EHR and PACS traffic
- 802.11r/k/v roaming for nurse mobility
- Audit-ready as-built documentation at project close

> **Clinical wireless failures are patient care disruptions — not ordinary IT tickets.**

BTI's Healthcare Wireless Engineering Methodology



Environments BTI Serves

Acute Care	Ambulatory Clinics	Specialty Practices	Behavioral Health
Long-Term Care			

Architecture Standards

- VLAN segmentation for clinical, IoT, and guest traffic
- Encrypted wireless (WPA3)
- Role-based access controls
- Centralized Meraki management

Compliance Deliverables

- As-built diagrams and AP placement records
- HIPAA Security Rule documentation
- Cyber insurance segmentation evidence
- Post-deployment validation report

> HIPAA compliance is not a configuration — it is an architecture. BTI builds it in from day one.

Request a Healthcare Infrastructure Assessment → btigroup.com

Branch Networks Built for Regulated Operations

PCI-DSS, SOX, and state financial regulations require encrypted, monitored, policy-enforced branch connectivity — and the ability to prove compliance on demand.

Legacy Branch Costs

- MPLS costs SD-WAN can reduce by 30–40%
- Configuration drift across 10+ branch locations
- Audit failures from inconsistent security policies
- Cyber insurance increases from undocumented segmentation
- No WAN failover or branch continuity path
- No centralized policy enforcement

What BTI Delivers

- SD-WAN with centralized policy enforcement and WAN failover
- Zero Trust branch access with identity-based controls
- Encrypted branch communications across all locations
- PCI-DSS segmentation with compliance evidence generation
- SOX-aligned change management and audit-ready documentation
- Meraki dashboard for real-time branch visibility

30–40%

WAN cost reduction

via SD-WAN vs. MPLS

—

PCI-DSS

Compliant segmentation and access controls

Zero Trust

Identity-based access and encrypted connectivity

> **In financial services, a branch network failure is a regulatory event, a customer trust failure, and an audit finding — often simultaneously.**

How BTI Modernizes Financial Branch Infrastructure

Secure Branch

Compliance Design

Redundant WAN

Centralized Management

What BTI Deploys

- **Cisco SD-WAN replacing legacy MPLS**
- **Meraki branch switching with centralized management**
- **Zero Trust Access via Cisco Duo MFA**
- **Encrypted branch-to-branch connectivity**
- **Consistent security policy across all locations**

Compliance Deliverables

- **PCI-DSS segmentation diagrams and evidence**
- **SOX change management records**
- **Cyber insurance segmentation documentation**
- **Audit-ready network diagrams**
- **Post-deployment validation reports**

30–40%

WAN cost reduction

via SD-WAN vs. legacy MPLS

PCI-DSS

PCI-DSS

Compliant segmentation and access controls

Zero-Trust

Zero-Trust

Identity-based access and encrypted connectivity

> **Operational continuity is engineered — not assumed.**

Schedule a Confidential Financial Infrastructure Assessment → btigroup.com

Campus Wireless for Every Device, Every Classroom

K-12 and higher education networks must support hundreds of simultaneous devices per building — students, faculty, IoT, safety systems, and administrative traffic — all on the same infrastructure.

Why Campus Wireless Deployments Fail

- AP density designed for average occupancy, not peak classroom or lecture hall load
- No roaming optimization between buildings — sticky client behavior across campus
- Student, faculty, and IoT devices on the same unsegmented network
- Standardized testing bandwidth demand overwhelming under-provisioned infrastructure
- Poor channel planning in multi-story and high-density buildings
- Outdoor coverage gaps breaking roaming between buildings
- E-Rate procurement delays from unfamiliar partners

What BTI Delivers for Education

- Ekahau RF modeling for peak classroom, lecture hall, and dormitory density
- Seamless roaming across buildings, outdoor areas, and multi-story environments
- Separate VLANs for student, faculty, IoT, guest, and safety communications
- Bandwidth planning for standardized testing and concurrent device saturation
- Campus safety integration — IP surveillance, VoIP, and emergency communications
- E-Rate eligible Cisco Meraki procurement with application guidance
- Centralized Meraki dashboard management across all campuses

> **A single poorly designed wireless environment can disrupt an entire school day — and a poorly planned deployment can fail an entire district.**

What BTI Delivers for K-12 and Higher Education

K-12 Districts

- High-density classroom wireless for 1:1 device programs
- Separate student, staff, IoT, and guest network segments
- Bandwidth provisioning for standardized testing windows
- E-Rate eligible Cisco Meraki procurement and guidance
- IP surveillance and emergency communications integration
- Centralized management across all district campuses

Higher Education

- Lecture hall and auditorium high-density wireless design
- Dormitory wireless density for student device saturation
- Seamless outdoor roaming across buildings and quads
- Research network segmentation and isolation
- Guest and conference wireless management
- Wi-Fi 6/6E for high-device-density environments

High-Density Wireless

Ekahau RF modeling and Wi-Fi 6/6E for peak occupancy and seamless roaming

Network Segmentation

Separate VLANs for student, faculty, IoT, and safety traffic

E-Rate Support

Procurement guidance to maximize federal funding for eligible Cisco Meraki infrastructure

Campus Safety

IP surveillance, VoIP, and emergency communications on the network

> **E-Rate funding can offset a significant portion of campus wireless costs — BTI navigates the program from application through procurement.**

Explore Campus Wireless Solutions → btigroup.com

Identity Verification

Device Trust

Network Segmentation

Application Access

Continuous Monitoring

Compliance Evidence

Network Architecture Is Now a Cybersecurity Decision

In 2026, network segmentation is an insurance requirement — not a best practice. Policies won't renew without documented evidence.

Architecture Checklist

- Segmentation documented for insurance validation
- Lateral movement contained
- MFA on remote access and privileged accounts
- Undocumented VLANs remediated
- SIEM active across all segments
- No EoL hardware in production

What BTI Can Deploy

- Zero Trust via Cisco Duo or other MFA
- VLAN segmentation with lateral movement containment
- Privileged access governance
- Segmentation evidence for insurance validation
- SIEM and log management integration
- Audit-ready compliance documentation

Cyber Insurance Risks

- Flat network — unrestricted lateral movement
- No MFA on remote or admin access
- Undocumented VLAN exposure
- Guest and corporate on shared segments
- EoL hardware with active CVEs

> **Segmentation is now an insurance requirement. Architecture is the control layer that turns policy into proof.**

Request a Cybersecurity Infrastructure Review → btigroup.com

Zero Dead Zones. 24/7 Fulfillment.

A dropped connection for a forklift scanner or AGV is immediate throughput failure — high ceilings, metal racking, cold storage, and dock environments defeat standard wireless designs.

Why Warehouse Wireless Fails

- AP placement from floor plans, not physical surveys with racking in place
- Forklift roaming transitions dropping sessions at aisle intersections
- Handheld scanner disconnects from sticky client behavior
- Dock door roaming failures between interior and exterior zones
- Cold storage RF reflection and compressor motor interference
- AGV coverage gaps breaking automated route continuity
- Telemetry traffic competing with scanner and automation workloads

What BTI Delivers

- Physical RF survey with racking and equipment in place
- 802.11r fast transition for forklift and AGV roaming
- Dock door and cold storage zone RF engineering
- AP power calibrated for aisle-level scanner reliability
- Separate VLANs for telemetry, automation, and scanner traffic
- Wi-Fi 6/6E for high-density concurrent device load
- Post-deployment validation before go-live sign-off

> **Warehouse wireless failures are throughput failures. BTI designs for 24/7 uptime — not average availability.**

BTI's Warehouse Wireless Engineering Process

RF Survey

Predictive Modeling

Roaming Analysis

Post-Deployment Validation

Lifecycle Support

Warehouse Wi-Fi / Ekahau predictive modeling and on-site surveys with racking in place — optimized for high-bay, cold storage, and dock environments.

OT/IoT Segmentation / WMS, conveyor controls, and IoT sensors isolated from corporate IT with full operational visibility.

SD-WAN Resilience / Multi-site WAN with automatic failover for distribution centers that cannot afford connectivity gaps.

Environments BTI Engineers

- High-bay distribution centers
- Cold storage and refrigerated facilities
- Dock and yard management areas
- Multi-building campus logistics
- Cross-dock and sortation facilities

What BTI Validates Before Go-Live

- Scanner uptime across all aisle transitions
- Forklift terminal roaming performance
- Cold storage zone RF coverage
- Dock door connectivity under load
- Channel utilization and interference levels

> "BTI conducts every warehouse RF survey with racking and inventory in place — not from a floor plan."

Request a Warehouse Wireless Assessment → btigroup.com

IT/OT Convergence Without Compromising Production

OT systems never designed for network exposure now share infrastructure with corporate IT — on a flat network, a single ransomware event becomes a production outage.

What Goes Wrong

- No PLC segmentation — industrial controls on the same segment as corporate IT
- SCADA and industrial IoT exposed to lateral movement
- Enterprise APs deployed without industrial RF survey
- AGV roaming gaps breaking automated production routes
- Plant floor RF interference from motors, welders, and metal structures
- No OT segmentation documentation for cyber insurance or NIST compliance

What BTI Delivers

- PLC and SCADA segmentation — industrial controls isolated from corporate IT
- Industrial IoT isolation with dedicated VLANs for sensors and automation
- OT ransomware containment — breach cannot propagate to production systems
- AGV roaming validation with 802.11r fast transition on production routes
- Plant floor RF survey for metal structures, motors, and interference sources
- NIST CSF segmentation documentation and audit-ready as-built records

What BTI Delivers for Manufacturing Environments

IT/OT Architecture

Converged segmentation isolating industrial controls from corporate IT.

Industrial Cybersecurity

NIST CSF and CIS framework-aligned security with OT-specific threat containment.

Plant Floor Wireless

Ekahau RF modeling for metal structures, moving equipment, and motor interference.

AI Analytics Readiness

Low-latency switching and wireless for real-time production monitoring and edge compute.

What BTI Segments

- Production and OT control systems
- Corporate IT and administrative traffic
- Industrial IoT and sensor networks
- Guest and contractor access
- Safety and emergency systems

Compliance Frameworks

- NIST Cybersecurity Framework
- CIS Controls
- IEC 62443 (Industrial Cybersecurity)
- Cyber insurance underwriter requirements

> **A properly segmented manufacturing network protects production, satisfies cyber insurance, and enables AI analytics — from the same infrastructure investment.**

Request a Manufacturing Infrastructure Assessment → btigroup.com

Public Sector Infrastructure Built for Accountability

Government agencies operate under strict security mandates, constrained IT staffing, and complex procurement requirements — while bearing direct responsibility for public safety communications and continuity of essential services.

Infrastructure Risks Unique to Public Sector

- **CJIS compliance gaps from undocumented or unaudited network segmentation**
- **Legacy switching in public safety facilities with no documented EOL remediation plan**
- **Shared network segments between public-facing services and internal government systems**
- **No redundant WAN or failover architecture for facilities supporting emergency response**
- **Grant funding opportunities missed due to unfamiliar or non-cooperative procurement partners**

> Infrastructure instability in government environments becomes a public safety issue — not merely an IT issue. Every unplanned outage in a dispatch center, public safety facility, or emergency communications network is a governance failure with real-world consequences.

What BTI Delivers for Public Sector Organizations

CJIS-Aware Network Design

Documented segmentation, access controls, and audit trails aligned to Criminal Justice Information Services compliance requirements.

Public Safety Continuity Architecture

Redundant WAN, automatic failover, and recovery procedures engineered for dispatch centers, EOC facilities, and emergency communications.

Grant-Aligned Modernization Planning

BTI aligns infrastructure investments with BEAD, E-Rate, COPS, and other grant programs — with documentation packages procurement offices can act on.

Procurement-Ready Project Delivery

Structured SOWs, milestone-based delivery, and full documentation packages that satisfy public sector audit and accountability requirements.

Physical Security Integration / IP surveillance, access control, and emergency communications on a unified, segmented infrastructure — one accountable partner, one documented architecture.

Multi-Site Governance / Centralized Meraki dashboard management across city halls, public safety facilities, libraries, and utility sites — with role-based access and change logging.

Agencies BTI Serves

- Municipal IT and city government
- Law enforcement and public safety agencies
- Emergency communications and dispatch centers
- School districts, libraries, and community services
- Water, utility, and special districts

Cooperative Procurement Vehicles

- TIPS / TASB Cooperative Purchasing (no separate RFP required)
- GSA Schedule-aligned procurement capability
- Grant-funded infrastructure program support
- ISNetworld certified contractor
- Compliant with public sector bid and audit requirements

BTI delivers infrastructure that is accountable, documented, and resilient — with procurement vehicles that eliminate barriers and project delivery that satisfies public sector audit requirements.

Request a Government Infrastructure Assessment → btigroup.com

AI Workloads Fail at the Network Layer

Most AI infrastructure failures begin at the network layer — not the application layer. Bandwidth saturation, uplink congestion, inference latency, and PoE budget shortfalls stop AI deployments before the algorithms ever run.

Four Infrastructure Realities of AI Deployment

1

AI Video Analytics Bandwidth

4K camera streams require 15–25 Mbps of consistent, prioritized throughput per camera. A 32-camera deployment can saturate a 1G uplink without proper QoS and uplink capacity planning.

2

Inference Latency Thresholds

Branch AI inference requires LAN latency under 5ms and WAN under 50ms. Without SD-WAN traffic prioritization, general user traffic competes directly with AI pipelines.

3

Edge Compute Placement

Local AI inference reduces cloud dependency and latency. Cisco Catalyst switching and Meraki wireless must be sized for edge GPU power draw and high-density PoE requirements.

4

Telemetry & Visibility

AI pipeline bottlenecks are invisible without network telemetry. Meraki and Catalyst Center provide the traffic visibility needed to detect congestion, latency spikes, and uplink saturation in real time.

⚠ Common AI Infrastructure Failure Points

- Uplink congestion from unsegmented AI and user traffic
- Switching capacity insufficient for AI pipeline throughput at peak load
- WAN latency exceeding inference thresholds without SD-WAN prioritization
- No telemetry — AI blind spots and bottlenecks go undetected
- PoE budget shortfalls blocking edge GPU and camera deployments
- Flat network architecture exposing AI systems to lateral movement

How BTI Engineers AI-Ready Infrastructure

BTI treats AI infrastructure as an engineering problem — not a product sale. Every engagement begins with a readiness assessment covering bandwidth, latency baselines, segmentation, PoE budgets, and telemetry before any device is procured.

Pre-Deployment Readiness Checklist

- Switching fabric supports AI pipeline throughput at peak load
- LAN latency under 5ms for real-time inference workloads
- AI workloads segmented from user and guest traffic
- Telemetry tools in place to surface bottlenecks and PoE oversubscription
- PoE budget sized for edge GPU and high-density camera deployments

Common Failure Points

- Uplink congestion from unsegmented AI and user traffic
- Switching capacity insufficient at peak AI pipeline load
- WAN latency exceeding inference thresholds without SD-WAN
- No telemetry — bottlenecks and blind spots go undetected
- PoE shortfalls blocking edge GPU and camera deployments

What BTI Delivers for AI Infrastructure

Bandwidth & Uplink Capacity Planning

Switching fabric sizing, uplink analysis, and QoS policy design for AI video analytics and inference.

Latency Baseline & SD-WAN Prioritization

LAN/WAN latency profiling with SD-WAN policies that protect AI pipelines from general user contention.

Edge Compute & PoE Architecture

Edge GPU placement planning and PoE budget analysis for high-density AI deployments.

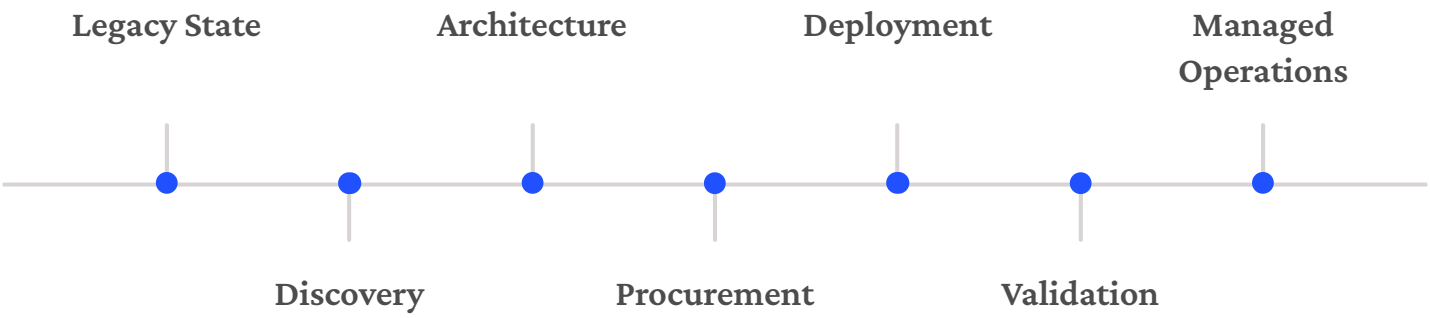
Telemetry & Visibility Engineering

Meraki and Catalyst Center telemetry for real-time visibility into AI pipeline performance and congestion.

Request an AI Infrastructure Readiness Assessment → btigroup.com

End-to-End. Every Phase. No Handoffs.

BTI executes every phase of the infrastructure lifecycle — from discovery through procurement, deployment, and managed operations — with no handoffs between teams.



What Every Assessment Includes

1	2
Infrastructure Inventory Switching, wireless, and WAN lifecycle status	**Wireless Heat Mapping** Ekahau-based coverage and AP placement
3	**4**
Risk Prioritization Findings ranked by operational and compliance impact	**Compliance Gap Analysis** HIPAA, NIST, CIS, PCI-DSS as applicable

Common Upgrade Mistakes

- Skipping assessment and going straight to procurement
- No wireless heat map or WAN topology review
- No cutover plan or rollback procedures
- Deploying without documentation

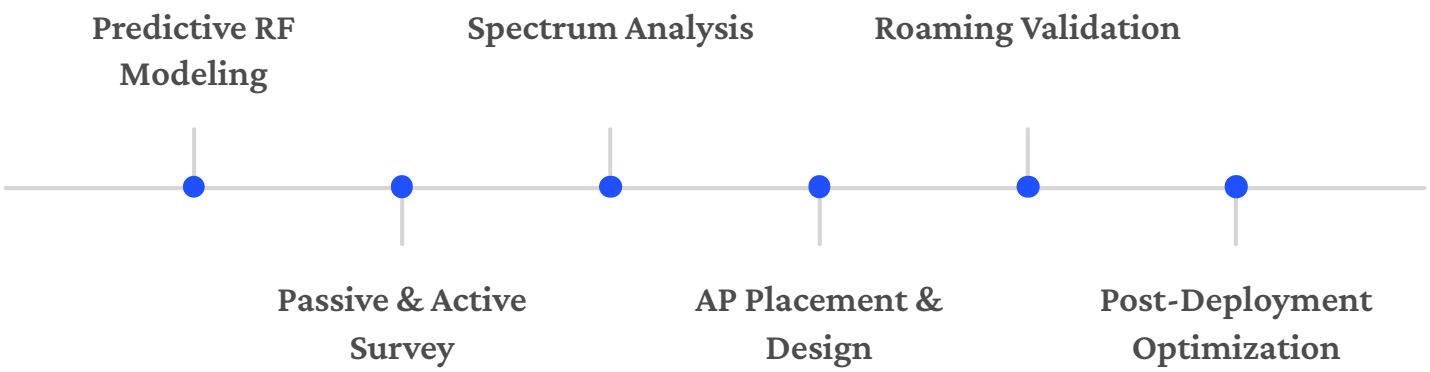
BTI's Ideal Delivery Standards

- Cutover and rollback plan (where applicable)
- Post-deployment validation and optimization
- Documentation delivered at project close
- Single point of accountability from assessment to go-live and support

Schedule a BTI Infrastructure Assessment → btigroup.com

Enterprise Wireless Engineering: Why RF Design Matters

Wireless performance problems are usually RF design problems — not hardware failures.



RF Problems BTI Resolves

Co-Channel Interference

Ekahau-modeled channel planning and transmit power optimization

Sticky Client Behavior

BSS transition configuration and roaming threshold tuning

AP Oversubscription

Ekahau capacity modeling during predictive design phase

Wireless Lifecycle Management

RF Validation & Benchmarking

Post-deployment active surveys confirm coverage, SNR, roaming, and throughput

Spectrum & Interference Analysis

Identifies Bluetooth, DECT, microwave, and rogue device interference

Firmware & Configuration Governance

Scheduled Meraki updates, channel plan reviews, and power adjustments

BTI uses Ekahau Pro for predictive design, active/passive survey, and post-deployment validation on every engagement.

Request a Wireless Site Survey → btigroup.com

Regional Presence. On-Site Expertise.

BTI maintains operational presence across Southern California, the Inland Empire, Orange County, Phoenix, and Chicagoland — with local project managers, on-site assessment teams, and regional logistics capability.

RF Surveys Require Physical Access

Wireless heat mapping cannot be done remotely — BTI can conduct Ekahau surveys at every facility.

Cutover Execution Requires On-Site Teams

Network migrations and cutover validation usually require physical presence at every critical deployment phase.

Compliance Documentation Requires Site Knowledge

Audit-ready documentation reflects the actual deployed environment — accuracy requires engineers on-site.

Southern California & Orange County

Los Angeles · Long Beach · Irvine · Anaheim · Costa Mesa

Inland Empire

Ontario · Rancho Cucamonga · Riverside · San Bernardino

Phoenix & Chicagoland

Mesa · Scottsdale · Tempe · Naperville · Oak Brook · Schaumburg

⚠ What Remote-Only Partners Miss

- RF interference only visible during a physical site walk
- Cabling and rack conditions affecting upgrade planning
- Operational workflow patterns informing AP placement
- Local compliance and installation constraints

> Every infrastructure assessment should include a physical site visit — not a remote questionnaire.

Contact Your Regional BTI Team → btigroup.com

Infrastructure Modernization in Action

These outcomes reflect BTI's operational delivery across regional, multi-site engagements.

14-Site Healthcare Network

Cisco Catalyst + Meraki wireless across 14 sites with centralized management and segmentation — HIPAA audit prep time cut by 60%.

Distribution Center Wireless

Meraki Wi-Fi 6 redesign after heat map survey — 99.97% scanner uptime and 18% pick rate improvement.

Manufacturing OT Segmentation

Cisco-based OT/IT segmentation with dedicated VLANs — satisfied cyber insurance requirements.

22-Branch SD-WAN Deployment

Cisco SD-WAN with centralized policy control — 34% WAN cost reduction and 99.99% availability.

60%

HIPAA Audit Prep Time Saved

99.97%

Scanner Uptime Achieved

34%

WAN Cost Reduction

18%

Warehouse Efficiency Gain

> Assess first. Design for the actual environment. Execute with governance. Document everything.

Start Your Modernization Conversation → btigroup.com

The Converged Infrastructure Advantage

Most vendors install infrastructure. BTI engineers accountable operational environments — converging IT, cybersecurity, physical security, and VoIP under one partner, one architecture, and one lifecycle.

Converged IT + Security + Physical Security + VoIP

One partner across network, cybersecurity, IP surveillance, access control, and unified communications.

PMO-Governed Execution

Milestone-based delivery, QA/QC checkpoints, and as-built documentation on every engagement.

ISO 27001 Operational Maturity

BTI's security management practices align to ISO 27001 — compliance is built in, not bolted on.

Lifecycle Accountability

Assess → Design → Procure → Deploy → Validate → Manage. No handoffs. No gaps.

BTI

- Converged IT + Cybersecurity + Physical Security + VoIP
- PMO-governed delivery with milestone documentation
- ISO 27001-aligned operational maturity
- ISNetworld certified — TIPS/TASB & GSA procurement
- Lifecycle ownership from assessment to managed operations

Generic VARs & MSPs

- Single-discipline focus — no converged delivery
- Reactive break-fix or ticket-based model
- No PMO governance or milestone accountability
- No cooperative purchasing vehicles
- Handoffs between vendors at every phase

Explore the Converged Infrastructure Model → btigroup.com

Infrastructure-Led Managed IT

Traditional managed IT focuses on resolving tickets after problems occur. BTI's infrastructure-led model prevents incidents by governing the underlying systems that cause them — with proactive governance, integrated cybersecurity, and compliance documentation built in by default.

What Infrastructure-Led Managed IT Means in Practice

Integrated Cybersecurity by Default

Cybersecurity monitoring, endpoint protection, and identity management integrated into infrastructure — not added after an incident.

Compliance-Ready Documentation

Audit-ready documentation and third-party audit support are standard practice — not reactive deliverables.

Infrastructure Risk Remediation

BTI remediates infrastructure risk before onboarding — not after the first outage. Risk metrics replace ticket metrics.

Unified Governance Across All Systems

Cloud, on-premises, IoT, VoIP, and physical security governed as one system — eliminating fragmented vendor gaps.

Proactive, Not Reactive

BTI governs infrastructure before incidents occur — not after tickets are opened. Risk metrics replace ticket volume as the measure of success.

Assessment Before Onboarding

Every engagement begins with an infrastructure risk assessment — identifying gaps in switching, wireless, segmentation, and compliance posture before work begins.

Single Accountable Partner

One partner governs IT, cybersecurity, physical security, and VoIP — eliminating the finger-pointing and coverage gaps of fragmented vendor relationships.

Infrastructure-Led vs. Traditional Managed IT

Understanding the distinction between traditional managed service providers and infrastructure-led models is critical for enterprise IT decision-makers. The differences extend beyond service scope — they reflect fundamentally different approaches to risk, liability, and operational accountability.

Capability Comparison

Capability	Traditional MSP	BTI Infrastructure-Led
Helpdesk Support	Primary focus	Included service
Infrastructure Remediation	Reactive or limited	Core responsibility
Cybersecurity Integration	Add-on service	Integrated by default
Compliance Governance	Minimal or absent	Built-in framework
Audit Documentation	Rarely maintained	Standard practice
Third-Party Testing Support	Not supported	Actively supported
Liability Alignment	Not addressed	Explicitly addressed

The Cost of Reactive IT Management

Compliance Exposure

Organizations without documented infrastructure controls face regulatory penalties, failed audits, and cyber insurance denials — all preventable with proactive governance.

Unresolved Infrastructure Debt

Reactive MSPs address symptoms, not root causes. Aging switching, undocumented segmentation, and firmware gaps accumulate until they become outages.

Fragmented Vendor Accountability

When IT, security, and voice are managed by separate vendors, no single party owns the outcome — and gaps between them become the client's problem.

Liability Without Documentation

Without audit-ready documentation, organizations have no evidence of reasonable controls — increasing legal and regulatory exposure after an incident.

Who Infrastructure-Led Managed IT Is For

Infrastructure-led managed IT is not the right model for every organization — it is the right model for organizations where IT failure creates regulatory exposure, operational disruption, or legal liability.

Organizational Fit

Best Suited For

- Multi-location or distributed operations
- Regulated consumer or employee data environments
- Cyber-insurance compliance requirements
- Converged IT, security, and voice environments
- Organizations where IT failure creates regulatory exposure

Risk of Staying with a Small MSP

- Compliance gaps from reactive-only infrastructure management
- Cyber insurance denials from undocumented controls
- Regulatory penalties from unmanaged risk exposure
- Operational outages from unresolved infrastructure debt
- Legal liability from absence of governance documentation

What BTI Assesses Before Every Engagement

- **Switching lifecycle status and segmentation architecture**
- **Wireless coverage, capacity, and roaming performance**
- **WAN resilience, latency baselines, and SD-WAN readiness**
- **Compliance posture against HIPAA, NIST, CIS, or PCI-DSS as applicable**
- **Cybersecurity controls, endpoint protection, and identity management gaps**

Request an Infrastructure-Led Managed IT Assessment → btigroup.com

Converged Infrastructure, Security & Governance

Infrastructure-led managed IT governs IT, cybersecurity, voice, and physical security as one converged system — eliminating the compliance gaps and operational exposures created by fragmented vendors.

The Four Converged Systems BTI Governs

IT Infrastructure

Cloud, on-premises servers, virtualization, storage, backup, and disaster recovery — governed proactively.

Cybersecurity

Threat monitoring, identity management, endpoint protection, and incident response — integrated by default.

Voice & Communications

VoIP, unified communications, contact centers, and collaboration — managed as infrastructure, not separately.

Physical Security

IoT devices, access control, IP surveillance, and environmental monitoring — governed within the same framework.

35+

Years of Proven Expertise

15+

Industries Served

10,000+

Alerts Handled, Zero Missed

Procurement Vehicles

GSA approved · CMAS contract holder · TIPS/TASB cooperative purchasing · TESMA — Los Angeles County · No separate RFP required.

Operational Credentials

ISNetworld certified contractor · ISO 27001-aligned practices · Cyber insurance compliance documentation · Third-party audit support standard.

Request an Infrastructure-Led Managed IT Assessment → btigroup.com

Five Principles for 2026 Infrastructure Decisions

Infrastructure Is Now a Cybersecurity Decision

Every switching, wireless, and WAN decision is simultaneously a security decision — flat networks are cybersecurity liabilities.

AI Readiness Begins at the Network Layer

AI workloads fail when the network isn't built to support them — low-latency switching and segmented wireless are prerequisites.

Segmentation Is No Longer Optional

Required for cyber insurance eligibility, regulatory compliance, and ransomware containment.

Operational Continuity Requires Lifecycle Management

Firmware governance, license renewal, and capacity planning separate resilient organizations from reactive ones.

Converged Accountability Reduces Risk

A single accountable partner with PMO discipline reduces operational risk and makes compliance manageable.

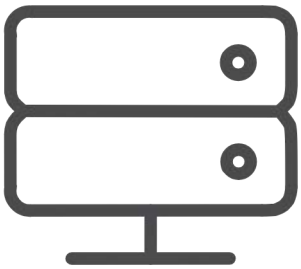
Request a BTI Infrastructure Assessment → btigroup.com

BTI Infrastructure Modernization Capabilities

BTI Communications Group delivers full lifecycle infrastructure modernization across Cisco networking, Cisco Meraki wireless, SD-WAN, cybersecurity, compliance, physical security, VoIP, and managed IT. Use this directory to explore the BTI service areas most relevant to your infrastructure modernization roadmap.

Cisco & Meraki Infrastructure

- Cisco Partner
- Cisco Meraki Partner
- Commercial Wi-Fi Installer
- Network Design
- Network Installation

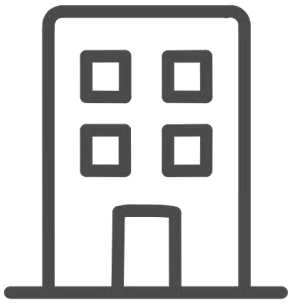


Infrastructure & Managed IT

- Infrastructure Consulting
- Infrastructure-Led Managed IT
- Managed IT Services

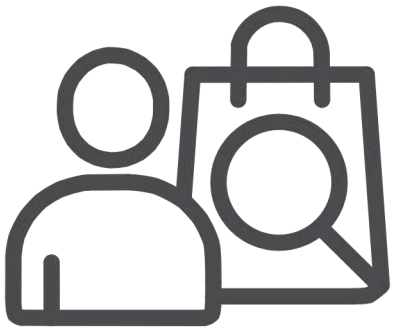
Cybersecurity, Compliance & Risk

- Cybersecurity Services
- Network Security
- Governance, Risk & Compliance



Converged Security & Communications

- Converged Security
- Physical Security Integration
- VoIP Installation



Public Sector & Procurement

- GSA Procurement Information
- Contact BTI

GSA approved contractor · CMAS contract holder · TIPS/TASB cooperative purchasing · ISNetworld certified

One Partner. One Operational Model.

Cisco, Meraki, cybersecurity, physical security, VoIP, and managed IT — designed, deployed, secured, and supported by BTI.

800-HELP-BTI · info@btigroup.com · btigroup.com

The Infrastructure Decision Is Already Overdue

Organizations that deferred switching refresh, wireless upgrades, and segmentation work in 2024–2025 are now one failure away from a compliance event, a ransomware exposure, or an AI deployment that cannot launch. Infrastructure modernization deferred too long eventually becomes operational recovery.

Cisco End-of-Support Exposure

Switching past end-of-support receives no security patches — every unpatched CVE is an open liability for cyber insurance and regulatory audits.

Wireless Performance Debt

Persistent wireless complaints that survive multiple AP replacements are RF design failures — not hardware failures. They will not resolve without a proper survey and redesign.

Cyber Insurance Renewal Pressure

Insurers now require documented segmentation, endpoint controls, and access governance — organizations without them face coverage denial or premium increases.

AI Readiness Blocked at the Network Layer

AI and automation initiatives stall when the underlying network cannot support inference latency, bandwidth requirements, or edge compute PoE demands.

Fragmented Vendor Accountability

Multi-site operations managed by separate IT, security, and voice vendors have no single party accountable for operational continuity — gaps between vendors become the organization's problem.

Undocumented Infrastructure

Network diagrams last updated more than 18 months ago are not documentation — they are a liability in any audit, incident response, or insurance claim.

Infrastructure Assessment

Switching, wireless, WAN, segmentation, and compliance review — with a phased modernization roadmap.

Wireless Site Survey

On-site Ekahau heat mapping and coverage analysis by BTI engineers.

SD-WAN & Security Review

WAN architecture assessment for cost reduction, resilience, and Zero Trust readiness.

The window to act before a compliance event, coverage denial, or operational failure is narrowing. Act now and contact BTI today.

Contact BTI Communications Group — 800-HELP-BTI · info@btigroup.com · btigroup.com