EXECUTIVE GUIDE

Executive Technology Partner Evaluation Guide

How leadership teams can select an IT partner that improves uptime, accountability, security, and execution instead of simply closing tickets.

WHITEPAPER 01

BUILT FOR

CEOs, COOs, CFOs, IT directors, operations leaders, and executives evaluating a provider change.

OUTCOME

A sharper decision process for choosing a provider that can support day-to-day operations, major projects, cybersecurity, procurement, and growth.

USE THIS WHEN

Leadership is comparing providers, support models, accountability, and long-term fit before a contract decision.

WHY THIS WHITEPAPER MATTERS

Executive brief

The wrong IT partner does not fail all at once. They fail in small ways that become expensive: slow escalation, weak documentation, poor project follow-through, unclear ownership, inconsistent account management, and reactive security. This guide gives leadership teams a practical model for evaluating whether a provider can operate as a true technology partner.

Revenue continuity

Downtime, slow response, and repeat problems directly affect employees, customers, billing, and delivery.

Security accountability

A provider with weak governance may leave patching, identity, backups, endpoint protection, and incident response undefined.

Execution quality

Projects fail when scope, procurement, staging, scheduling, and handoff are not managed as one operating system.

Leadership visibility

Executives need reporting that explains risk, progress, cost, decisions, and tradeoffs without technical noise.

Leadership takeaway: A provider decision is an operating decision that affects reliability, security, cost, accountability, and business momentum.

COMMON FAILURE PATTERNS

Where organizations lose control

Provider issues rarely appear all at once. They build when ownership, documentation, escalation, and follow-through are unclear.

What to watch for

- The provider measures ticket closure but not repeat issue reduction, root cause removal, or business impact.
- Escalations depend on heroic individuals instead of a documented service model.
- Projects are sold separately from support, so handoffs break and no one owns the full outcome.
- Security tools exist, but governance, response roles, review cadence, and evidence are not clear.
- Procurement, device standards, and lifecycle planning are treated as afterthoughts.
- The executive sponsor only hears from the provider when something is broken or a renewal is due.

Operational truth: Control is proven by ownership, evidence, escalation, and repeatable execution - not by activity alone.

Impact if ignored

Small gaps become recurring tickets, missed handoffs, delayed projects, unclear security ownership, and leadership surprises.

Corrective move

Assign an owner, define the standard, require evidence, and review progress on a leadership cadence.

OPERATING MODEL

The HTG Partner Evaluation Model

A mature approach turns scattered activity into a repeatable system. Use this model to define ownership, sequence, quality checks, and handoff.

1

Stabilize

Inventory the environment, reduce recurring issues, document escalation paths, and establish a clean service baseline.

2

Secure

Build the practical security baseline: identity, endpoint, backups, patching, monitoring, user controls, and incident readiness.

3

Standardize

Define approved hardware, network, device, software, access, and vendor standards so the business can scale consistently.

4

Execute

Run projects with scope control, staging, scheduling, field coordination, quality checks, and post-project handoff.

5

Improve

Use reporting, QBRs, roadmaps, lifecycle planning, and budget conversations to keep the environment moving forward.

Execution rule: Do not move from one stage to the next until ownership, evidence, and acceptance criteria are clear.

01

Own the standard

Decide what good looks like before work begins.

02

Prove readiness

Verify facts before scheduling, buying, deploying, or closing.

03

Close the loop

Document outcomes so support and leadership can act.

STANDARDS THAT MAKE THE WORK REPEATABLE

What good looks like

A professional IT program does not rely on memory or individual heroics. It uses standards that make quality visible, measurable, and repeatable.

Standard area	Practical expectation
Service ownership	Clear intake, triage, escalation, SLA logic, root cause tracking, recurring issue reduction, and executive reporting.
Security baseline	MFA, endpoint protection, patching, backup review, monitoring, access review, vendor controls, and incident playbooks.
Project execution	Documented scope, procurement readiness, staging, field coordination, change control, and acceptance criteria.
Lifecycle planning	Asset inventory, warranty visibility, refresh roadmap, standard builds, secure retirement, and cost forecasting.
Leadership rhythm	QBRs that discuss risk, business priorities, roadmap progress, budget, and decisions needed.

Decision principle: Anything that cannot be documented, repeated, assigned, measured, or handed off will eventually become support debt.

Documented

The process is written and current.

Measured

Leadership can see trend and risk.

Owned

Someone is accountable for completion.

ACTIONS THAT CREATE REAL PROGRESS

Implementation playbook

Use these actions to move from vague concern to a practical operating plan. Each item should have an owner, due date, and evidence of completion.

- ✓ Run a provider scorecard before renewal or replacement conversations begin.
- ✓ Separate sales promises from delivery evidence; require proof of process, not only references.
- ✓ Look at procurement and lifecycle handling; device chaos usually becomes support chaos.
- ✓ Require a clean onboarding plan that includes discovery, documentation, access, tools, tickets, reporting, and leadership cadence.
- ✓ Ask for examples of operating reviews, project plans, security reports, and escalation documentation.
- ✓ Review the provider's documentation habits, because undocumented support does not scale.
- ✓ Confirm who owns security decisions, who monitors risk, and how incidents are handled.

Practical priority: Fix the facts first. Most technology programs improve faster once inventory, ownership, access, documentation, and acceptance criteria are clean.

HOW LEADERSHIP SHOULD TRACK IT

Governance and measurement

The right metrics make progress visible. The wrong metrics make a messy environment look busy. Leadership should track the signals that explain health, risk, and accountability.

Measurement area	What to track
Operational health	Ticket aging, repeat incidents, SLA performance, escalation patterns, user satisfaction, problem categories.
Security readiness	MFA coverage, endpoint coverage, patch posture, backup status, alert review, access review, incident exercises.
Project execution	Milestone completion, change orders, procurement readiness, field dispatch quality, acceptance defects.
Lifecycle control	Asset accuracy, warranty coverage, aging device count, refresh plan adherence, retired asset disposition.
Executive value	Roadmap completion, risk reduction, budget visibility, business priority alignment, QBR action closure.

Reporting rule: A leadership report should answer four questions: What changed? What risk remains? What decision is needed? What happens next?

Executive view

Show the top risks, blocked work, cost impact, and decisions due.

Operational view

Show work volume, aging, recurring issues, defects, and ownership.

USE THESE BEFORE APPROVAL

Executive decision questions

These questions are designed to expose weak assumptions before they become project delays, support issues, security gaps, budget surprises, or operational risk.

- ✓ What specific issues will you try to remove in the first 90 days, not just support?
- ✓ Who owns cybersecurity recommendations, incident escalation, and leadership communication?
- ✓ What does your QBR actually show beyond ticket counts?
- ✓ What would cause you to recommend replacing or standardizing technology?
- ✓ How do you document the environment, and how often is that documentation reviewed?
- ✓ How do procurement, imaging, staging, and device standards connect to support?
- ✓ How are projects transitioned back into support after completion?
- ✓ How do you handle multi-site, remote-user, and after-hours escalation needs?

What strong answers sound like

Strong answers include ownership, current state, target state, evidence, tradeoffs, timing, dependencies, and the decision leadership needs to make.

SCORE HONESTLY BEFORE INVESTING

Readiness scorecard

Rate each area from 1 to 5. A score of 1 means ad hoc and risky. A score of 3 means partially controlled. A score of 5 means documented, measured, reviewed, and repeatable.

1 **Strategic fit**
Provider understands business operations, risk tolerance, and growth plans.

2 **Operational discipline**
Provider has a documented service model and proves follow-through.

3 **Security maturity**
Provider can explain controls, monitoring, response, and gaps clearly.

4 **Project capability**
Provider can execute deployments, refreshes, moves, and multi-site work.

5 **Lifecycle control**
Provider helps plan purchases, standards, warranties, refreshes, and retirement.

6 **Executive communication**
Provider makes technology understandable and actionable for leadership.

Scoring rule: The overall score is not the average. The weakest critical area usually defines the real risk.

TURN THE GUIDE INTO MOVEMENT

30/60/90 action plan

A useful whitepaper should turn into execution. This plan gives leadership a practical starting point for improving control without overcomplicating the first step.

Days 1-30

Discovery, access cleanup, documentation, ticket review, tool coverage check, backup and endpoint baseline.

Days 31-60

Issue reduction plan, security gap priorities, procurement standards, lifecycle inventory, leadership reporting cadence.

Days 61-90

Roadmap, budget model, project backlog, recurring review rhythm, measurable improvement targets.

How HTG applies this in the real world

HTG helps organizations turn technology priorities into executable work: assessments, procurement, staging, managed services, cybersecurity readiness, lifecycle visibility, field execution, infrastructure projects, and leadership reporting.

Ready to turn this into a practical operating plan?

Use this guide as the starting point for a focused review of your environment, risk, priorities, projects, and next decisions.

TALK WITH HTG

ACCURACY AND PRACTICAL USE

Source-grounded notes and reference basis

This whitepaper is written for executive planning and practical operations. It uses recognized public guidance as a foundation where security, continuity, privacy, data protection, incident response, media sanitization, healthcare, financial safeguards, or payment security concepts are discussed.

- **NIST CSF 2.0:** National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, February 2024. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final
- **CISA CPG 2.0:** Cybersecurity and Infrastructure Security Agency, Cross-Sector Cybersecurity Performance Goals 2.0. https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0
- **CIS Controls v8.1:** Center for Internet Security, CIS Critical Security Controls Version 8.1. https://www.cisecurity.org/controls/v8-1
- **NIST IR:** National Institute of Standards and Technology, SP 800-61 Rev. 3, Incident Response Recommendations and Considerations. https://csrc.nist.gov/pubs/sp/800/61/r3/final
- **NIST Contingency:** National Institute of Standards and Technology, SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems. https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

Important: This guide is business guidance, not legal, compliance, insurance, or audit advice. Requirements vary by environment, contract, industry, cyber-insurance policy, and regulator. Use it to improve planning, then confirm obligations with the appropriate counsel, auditor, carrier, or compliance owner.

HTG closing standard

The best technology work is not merely installed. It is documented, governed, supported, measured, and improved.