READINESS ASSESSMENT

Business IT Readiness Assessment

A leadership scorecard for evaluating whether support, security, infrastructure, lifecycle, vendors, backups, and growth readiness are under control.

WHITEPAPER 07

BUILT FOR

Executives, owners, operations leaders, IT managers, finance leaders, and organizations preparing for growth, acquisition, or provider change.

OUTCOME

A practical view of where IT is stable, where risk is building, and what should be prioritized in the next 90 days.

USE THIS WHEN

Leadership wants a practical assessment before growth, budget planning, risk review, acquisition, or provider change.

WHY THIS WHITEPAPER MATTERS

Executive brief

Most businesses do not need a theoretical IT assessment. They need to know whether employees can work, systems can recover, security controls are real, vendors are controlled, assets are known, and leadership can make decisions before problems become expensive.

Employee productivity

Poor support, unstable devices, weak Wi-Fi, and recurring issues waste time every day.

Business risk

Security, backup, access, and vendor gaps can become incidents with operational and financial impact.

Growth readiness

A business cannot scale cleanly with undocumented systems, inconsistent onboarding, and reactive purchasing.

Decision quality

Leadership needs a clear roadmap instead of disconnected technical complaints.

Leadership takeaway: IT readiness gives leaders a clearer view of what is stable, what is fragile, and what needs attention before growth adds pressure.

COMMON FAILURE PATTERNS

Where organizations lose control

Readiness gaps often stay hidden until growth, turnover, outages, audits, or provider transitions expose them.

What to watch for

- IT is judged only by whether tickets are answered, not whether the environment is improving.
- Business-critical systems are not ranked by operational impact or recovery priority.
- User onboarding and offboarding depend on memory, causing access gaps and inconsistency.
- Vendors have access, but no one regularly reviews what they can reach or why.
- Backup success is assumed from reports but not proven through restoration testing.
- There is no 90-day roadmap that connects risk, budget, projects, and accountability.

Operational truth: A mature IT environment can explain its risks, owners, standards, systems, and priorities without relying on memory.

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 Seven-Part IT Readiness Model

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

1
Support
Ticket intake, escalation, documentation, root cause, and user experience.

2
Security
Identity, endpoint, email, patching, monitoring, backups, and incident readiness.

3
Infrastructure
Network, Wi-Fi, firewalls, switching, cloud systems, servers, and connectivity.

4
Lifecycle
Procurement, standards, asset inventory, warranty, refresh, and retirement.

5
Vendors
Contracts, access, escalation contacts, renewals, service ownership, and risk.

6
Recovery
Backup, restore testing, critical systems, RTO/RPO, and continuity actions.

7
Roadmap
Budget, projects, priorities, dependencies, and executive reporting.

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
Support readiness	Documented intake, escalation, response expectations, recurring issue tracking, and ownership.
Security readiness	MFA, endpoint protection, patching, access review, backup protection, and alert handling.
Infrastructure readiness	Stable network, reliable Wi-Fi, documented ISP/failover, equipment lifecycle, and site diagrams.
Lifecycle readiness	Accurate assets, approved standards, refresh plan, warranty visibility, and secure retirement.
Leadership readiness	Roadmap, budget forecast, risk ranking, QBR rhythm, and decision log.

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.

- ✓ Score the environment honestly; do not average away critical weaknesses.
- ✓ Rank gaps by business impact, likelihood, and effort to correct.
- ✓ Create a 90-day plan that leadership can understand and fund.
- ✓ Review readiness quarterly so improvements do not disappear after the assessment.
- ✓ Start with systems that stop the business if they fail.
- ✓ Separate urgent fixes from roadmap improvements.
- ✓ Assign an owner and due date to every important gap.

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
Support	Open ticket aging, repeat issue rate, user satisfaction, escalation performance.
Security	MFA coverage, endpoint coverage, patch compliance, admin/stale accounts, alert ownership.
Infrastructure	ISP uptime, Wi-Fi issues, network equipment age, documented topology, capacity constraints.
Lifecycle	Asset completeness, warranty status, refresh backlog, unknown devices, retired equipment backlog.
Recovery	Backup success, restore test date, RTO/RPO alignment, critical system runbooks.

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 systems would stop revenue, service delivery, patient/customer experience, or payroll if unavailable?
- ✓ Do we know who has access to what, including vendors and former employees?
- ✓ What equipment is aging, unsupported, out of warranty, or not documented?
- ✓ Where is IT slowing growth, onboarding, expansion, or project execution?
- ✓ What support issues repeat every month, and why have they not been removed?
- ✓ Can we restore the systems that matter most within the timeframe the business expects?
- ✓ What does leadership need to fund, accept, or defer in the next 90 days?
- ✓ What proof do we have that controls are working?

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. **Support maturity**
   Support is organized, documented, measurable, and improving.
2. **Security baseline**
   Foundational controls are enforced, monitored, and reviewed.
3. **Infrastructure stability**
   Connectivity, network, and core platforms are documented and reliable.
4. **Lifecycle control**
   Assets are known, planned, supported, and retired properly.
5. **Vendor governance**
   Vendors, access, renewals, ownership, and escalation paths are controlled.
6. **Recovery confidence**
   Backups, priorities, and restoration capability are validated.
7. **Roadmap discipline**
   Leadership receives an actionable roadmap tied to risk and budget.

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

Assess support, security, infrastructure, backup, vendors, assets, and critical systems.

Days 31-60

Fix high-risk quick wins, document priorities, assign owners, and define roadmap categories.

Days 61-90

Create executive roadmap, budget model, QBR dashboard, and recurring readiness review cadence.

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 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
- **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

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.