singlepoint GLOBAL

2027 Is Calling for a Bolder Technology Playbook

What to Prioritize Before January and How to Strengthen Your IT Strategy for the Year Ahead.

Make the Most of the Time Before 2027

Budgets are being finalized, projects are moving into next year's calendar, and business leaders are deciding where to invest their resources. It's a valuable moment to ask whether the technology behind those plans is receiving the same attention as the plans themselves.

An infrastructure upgrade that keeps getting postponed, a cloud subscription that no longer delivers enough value, or a support arrangement that hasn't evolved with the business can all affect what happens next. Addressing these matters now gives your organization more control over how it enters 2027.

This guide will help you identify practical improvements, evaluate the resources available to your team, and make informed decisions about Managed IT and Co-Managed IT Services. The objective is to turn technology planning into measurable business progress, beginning with the decisions you can make today.

Put Recurring IT Problems Behind Your Business

A technology issue rarely stays within the IT department. When an essential application stops working, customer requests may be delayed, employees may need temporary workarounds, and managers may have to reorganize scheduled activities. Even after the system is restored, completing the interrupted work takes additional time.

For a business owner or operations director, the concern is not simply how quickly a ticket gets closed. It is how frequently these interruptions occur, which activities they affect, and whether the same problems continue returning. Those details help distinguish an isolated incident from a recurring operational weakness.

Identify Where Interruptions Affect Performance

Start by reviewing the incidents that required the most attention during 2026. Instead of treating every support request equally, examine the consequences for employees and customers.

Three areas deserve particular attention:



- **Workforce productivity:** Frequent connectivity problems, slow applications, and unreliable equipment can interrupt employees throughout the day. Identifying the systems involved helps determine where improvements could recover productive time.
- **Customer experience:** Delays in accessing records, processing transactions, or responding to requests may affect service quality. Understanding these dependencies helps establish which systems need the greatest reliability.
- **Project schedules:** Repeated troubleshooting can compete with planned upgrades and implementations. Reviewing postponed work reveals where operational issues have affected progress on business priorities.

This information provides a practical basis for determining what should change. It also helps leadership evaluate technology performance using business outcomes rather than relying exclusively on technical reports.

Make Prevention Part of Daily Operations

Regular monitoring, scheduled maintenance, and documented procedures help organizations manage systems more consistently. These practices can identify developing problems, establish appropriate upgrade schedules, and provide technicians with information that supports faster troubleshooting.

For example, monitoring may reveal that storage capacity is approaching a limit or that a network device is experiencing repeated performance issues. Addressing these conditions during a planned maintenance window is generally preferable to discovering them during an important business activity.

As you prepare for January, review which recurring problems could be reduced through better monitoring, maintenance, or infrastructure planning. This is a useful first step toward creating a more dependable operating environment.

Give Your 2027 Technology Budget a Clear Purpose

Financial planning becomes more difficult when technology spending is divided among subscriptions, equipment purchases, outside vendors, emergency services, and individual projects. Each expense may appear reasonable on its own, yet the combined cost can be difficult to evaluate without a complete view.

For CFOs and business owners, the objective is to understand what the organization is paying for and whether those investments continue to serve a business purpose. A lower monthly support fee may not represent better value if important services are excluded or additional technical work requires separate charges.

Review Spending Before Renewals Take Effect

Cloud environments provide a useful example. According to the Flexera 2026 State of the Cloud Report, organizations estimated that 29% of their infrastructure and platform cloud spending was wasted. This finding illustrates why businesses should regularly review resource utilization, subscription ownership, and service configurations.

The same principle applies to other technology expenses. Before approving the next annual budget, examine the following categories:

Spending Area	What to Review	Business Objective
Software and cloud services	Licenses, subscriptions, usage, and overlapping capabilities	Improve utilization and eliminate unnecessary expenses
Infrastructure	Equipment condition, warranties, and replacement schedules	Plan upgrades before performance becomes a concern
IT support	Service scope, response expectations, and additional charges	Understand the full cost of technical assistance
Security and recovery	Existing safeguards, backup arrangements, and identified gaps	Fund improvements according to business exposure
Strategic projects	Implementation requirements, external expertise, and timelines	Allocate resources before work begins

Evaluate the Return Beyond Cost Savings

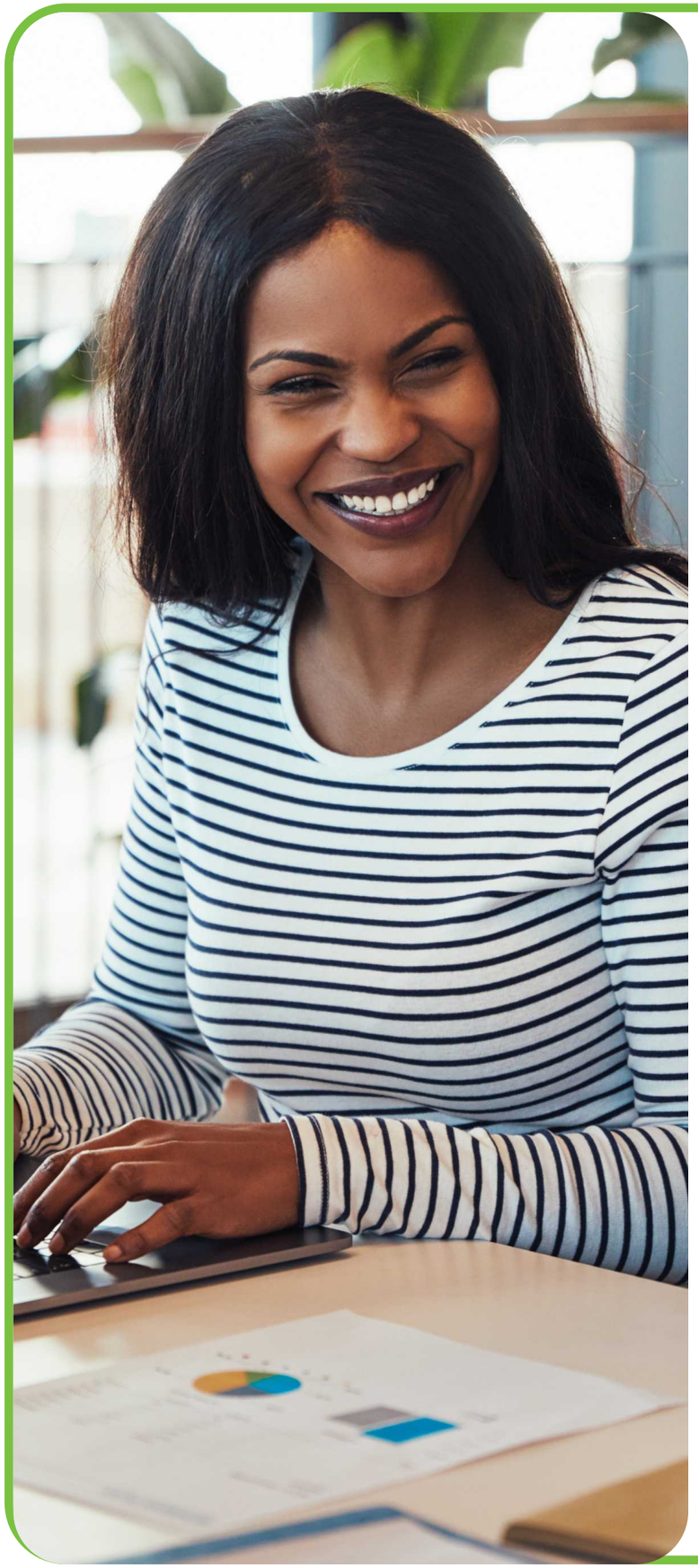
An effective investment does not always produce an immediate reduction in spending. Replacing an aging server may improve reliability. Strengthening identity controls can help protect sensitive information. Adding technical resources to a project may improve the organization's ability to meet an implementation deadline.

Each proposal should explain the problem being addressed, the expected result, and how progress will be measured. This makes it easier for leadership to compare competing priorities and determine which initiatives deserve funding.

The remaining weeks of 2026 are an opportunity to complete this review before new contracts and project commitments take effect.



Build confidence in what comes next.



Make Cybersecurity a Business Investment

Every new application, employee account, vendor connection, and cloud service introduces responsibilities that must be managed. Over time, permissions may become outdated, systems may receive inconsistent updates, and security procedures may no longer reflect how employees actually work.

These conditions can develop even in organizations with experienced technical professionals and established security tools. A useful security strategy therefore begins with understanding the environment and identifying which weaknesses could have the greatest operational consequences.

Focus on Access, Visibility, and Accountability

The Microsoft Digital Defense Report 2026 found that 52.2% of observed intrusions involving valid accounts included subsequent credential theft. This finding highlights the importance of protecting business identities and limiting unnecessary access.

For organizations reviewing their security arrangements, four areas provide a practical starting point:

- **Identity management:** Review user permissions, privileged accounts, and multifactor authentication. Ensure that access changes when employees change responsibilities or leave the organization.
- **System protection:** Maintain appropriate software updates, endpoint safeguards, and security configurations across business devices and applications.
- **Threat monitoring:** Establish procedures for identifying suspicious activity, investigating alerts, and escalating incidents to the appropriate personnel.
- **Security responsibilities:** Document who manages essential controls, approves changes, and coordinates responses when a potential issue is identified.

These activities help leadership understand whether existing safeguards are being maintained consistently and where additional expertise may be useful.

Prioritize the Improvements That Matter

A security review should produce a manageable list of actions rather than an extensive collection of recommendations without clear ownership. Start with systems that support essential operations, store sensitive information, or provide access to multiple business applications.

Then evaluate the likelihood and potential consequences of relevant threats, the effectiveness of existing safeguards, and the resources required for improvement.

This approach allows businesses to direct security investments toward defined needs. It also gives finance and executive leaders a clearer explanation of why particular controls deserve attention in the upcoming budget.

Know How Your Business Will Recover

An interruption can originate from many sources, including equipment failure, accidental deletion, cloud service problems, or a cybersecurity incident. While preventive measures reduce exposure, organizations also need a practical way to restore essential activities when normal operations are disrupted.

A business continuity plan should explain which processes take priority, how information will be recovered, and who will coordinate the response. Without those decisions, employees may spend valuable time determining what to do while customers and business activities are already affected.

Set Recovery Expectations Around Actual Needs

Not every application requires the same restoration timeframe. A customer transaction system may need to return quickly, while certain reporting tools can remain unavailable for longer without seriously affecting operations.

Two measures help organizations establish appropriate expectations:

- **Recovery Time Objective (RTO):** The target amount of time within which a system or process should be restored.
- **Recovery Point Objective (RPO):** The maximum acceptable period of data loss, based on the most recent recoverable information.

These requirements influence backup schedules, storage arrangements, recovery procedures, and infrastructure investments. They should be established with input from the departments that depend on each system.

Validate Your Recovery Procedures

A successful backup does not necessarily mean an organization can restore operations within its required timeframe. Testing should confirm that information can be recovered, applications function correctly, and employees have the access needed to resume their responsibilities.

According to PwC's 2027 Global Digital Trust Insights, only 39% of surveyed security, risk, and operations leaders had fully formalized and integrated operational continuity plans specifically addressing cyber risks.

The finding reinforces the importance of moving beyond documented intentions. Businesses should test their procedures, identify dependencies, and update recovery instructions when systems or responsibilities change.

Before 2027 begins, consider scheduling a recovery exercise for one of your most important applications. The results can help establish whether current arrangements meet business expectations or require further attention.

The right expertise. A shared direction.

Give Your Internal IT Team More Ways to Deliver

Internal technology professionals bring valuable knowledge to an organization. They understand existing systems, employee requirements, past implementation decisions, and the priorities of different departments. That experience provides an important foundation for evaluating new initiatives.

However, the resources required for an infrastructure upgrade or specialized security project may differ from those needed to manage daily operations. An experienced department can benefit from additional expertise without changing its leadership structure or transferring responsibility for every technical decision.

Match Additional Resources to Specific Projects

Consider a company preparing to migrate important applications to the cloud. Its internal team may understand the applications and business requirements, while outside specialists contribute migration planning, technical implementation, and configuration expertise.

A similar arrangement may help during network upgrades, security assessments, or periods when additional user support is required.

Co-Managed IT Services provide a framework for this collaboration. An external provider contributes agreed resources while the internal department continues directing the organization's technology priorities.

The arrangement should establish clear responsibilities, communication procedures, and escalation paths. This allows both teams to coordinate their work without duplicating tasks or creating uncertainty about ownership.

Use Specialized Expertise Where It Adds Value

Research from RSM's 2026 Cybersecurity Special Report found that U.S. middle-market organizations outsourced specialized security functions, including cloud security management, security awareness training, and security operations center services.

This demonstrates how external providers can contribute capabilities that complement an organization's existing resources.

For decision-makers, the relevant questions are practical: Which initiatives require additional skills? How long will those resources be needed? Would permanent hiring be appropriate, or could a defined external engagement provide a better fit?

Answering these questions helps businesses choose a staffing and support arrangement based on actual requirements rather than assumptions about what an internal department should handle independently.

Choose the IT Support Model That Fits Your Organization

Managed IT and Co-Managed IT Services offer different ways to organize technical responsibilities. The right approach depends on existing personnel, operational requirements, service expectations, and the level of involvement leadership wants from an outside provider.

A business without a dedicated internal department may prefer comprehensive technical management. An organization with experienced specialists may need additional coverage or project resources in selected areas.

Managed IT Services

A fully managed arrangement allows a provider to assume agreed responsibilities for ongoing technology operations. These may include monitoring, help desk assistance, network and cloud management, routine maintenance, and certain security activities.

The organization should understand which services are included, how requests are handled, and what responsibilities remain with internal personnel or other vendors.

Co-Managed IT Services

A co-managed arrangement supports an existing department by providing additional capabilities under a shared operating structure.

For example, an internal team may retain responsibility for business applications while the external provider assists with infrastructure monitoring, user support, or specialized projects. The division of work can reflect the organization's established processes and priorities.

Compare the Available Approaches

Decision Factor	Managed IT Services	Co-Managed IT Services
Primary purpose	Provide broad external management of technology operations	Complement an existing internal department
Daily support	Provider handles agreed operational responsibilities	Responsibilities are divided between both teams
Technical leadership	Provider works with business leadership on planning and execution	Internal IT retains a central role in directing priorities
Specialized resources	Available through the agreed service scope or additional projects	Added according to the team's specific requirements
Best starting question	Which functions should be managed externally?	Where would additional expertise improve execution?

The choice should also account for communication, reporting, service expectations, and how responsibilities may change as the organization evolves.

A productive provider relationship depends on more than technical capability. It requires a clear understanding of the business, consistent coordination, and accountability for agreed services.

Your 2027 Readiness Checklist

By this stage, the most useful next step is to translate the previous considerations into a focused review. Leadership does not need to resolve every technical issue before January, but it should know which matters require attention and who will be responsible for addressing them.

The following checklist can support a discussion among executive leadership, finance, operations, and IT.

Priority Area	Question to Answer	Recommended Action
Operational reliability	Which recurring issues affected productivity or customer service?	Review incident patterns and identify corrective measures
Financial planning	Are renewals, replacements, and planned projects reflected in the budget?	Consolidate technology expenses and upcoming commitments
Cybersecurity	Are essential access controls and safeguards being maintained?	Review security responsibilities and priority risks
Business continuity	Can important systems be restored within acceptable timeframes?	Validate recovery procedures and business requirements
Technical resources	Which upcoming initiatives require specialized skills or additional capacity?	Determine internal and external resource needs
Provider accountability	Are service responsibilities and escalation procedures clearly defined?	Review agreements and operational expectations



Turn clarity into forward momentum.

Turn Your Findings Into an Action Plan

A useful readiness review should conclude with a manageable sequence of activities. Begin by documenting the current environment and the business requirements for the coming year. Prioritize improvements according to their operational impact, then assign resources and establish realistic implementation schedules.

The following framework provides a straightforward structure:

ASSESS → PRIORITIZE → RESOURCE → EXECUTE → MEASURE

Assess: Review systems, contracts, recurring issues, security arrangements, and planned initiatives.

Prioritize: Determine which improvements deserve attention based on business consequences and implementation requirements.

Resource: Assign ownership, budgets, technical expertise, and any necessary outside assistance.

Execute: Schedule and deliver improvements while accounting for operational dependencies.

Measure: Evaluate whether the completed work produces the expected results and identify adjustments where necessary.

For example, a company preparing to open another location may need to evaluate connectivity, equipment requirements, cloud access, and employee support before the opening date. Establishing these requirements early gives the project team time to coordinate vendors, approve spending, and prepare the environment.

Three Commitments to Make Before January

As 2026 comes to a close, leadership can create meaningful progress by making three decisions:



Confirm immediate priorities: Agree on which improvements should be funded, scheduled, or investigated before new initiatives begin.



Establish clear ownership: Identify who will lead each activity and whether additional resources are required.



Schedule a progress review: Set an early 2027 meeting to evaluate implementation, spending, and emerging business needs.

These commitments create accountability and help the organization begin the new year with work already underway.

Bring Your 2027 Strategy Into Focus

A technology plan is most useful when it reflects the business it is intended to support. That requires an understanding of existing systems, employee needs, operational priorities, and the resources available to deliver improvements.

SinglePoint Global provides Managed IT and Co-Managed IT Services for organizations in Virginia and the surrounding region. Its capabilities include monitoring, help desk assistance, cybersecurity support, cloud and network management, and additional technical resources for internal departments.

The company's approach begins with reviewing the organization's technology environment, identifying areas that require attention, and determining which services fit its requirements. Businesses seeking comprehensive support can explore a managed arrangement, while those with established internal teams can consider a collaborative model.



Make Your Next Conversation About What Comes Next

You may already know which projects deserve attention in 2027. Perhaps a system needs upgrading, a security requirement needs addressing, or your internal team could benefit from specialized expertise for an upcoming initiative.

What matters now is turning those observations into a plan with clear priorities, appropriate resources, and realistic expectations.

SinglePoint Global can help you evaluate your current environment and explore the support arrangement that makes sense for your organization. The conversation can begin with the business objectives you want to achieve and the technical questions that need answers.

Your plans for 2027 are taking shape. Give them the technology strategy and resources to move forward.

LET'S PLAN YOUR NEXT MOVE WITH SINGLEPOINT GLOBAL

SinglePoint Global | Managed IT & Co-Managed IT Services


singlepoint
GLOBAL