balancelogic
THE ANSWER FOR SMALL BUSINESS.

2025

SMB

IT Planning Checklist

DATE :
July, 23, 20025

CREATED BY:
Bill Campbell, CISSP, CSCP

Table of Contents

1. Assess Your Current IT Infrastructure 3

Conduct a comprehensive IT Infrastructure Assessment 3
Identify scalability challenges and bottlenecks 3
Benchmark your systems against industry standards 3
Assess alignment with compliance frameworks (e.g., HIPAA, NIST) 3

2. Strengthen Cybersecurity Posture 3-4

Establish a cybersecurity framework tailored to your business 3
Deploy and maintain security tools (firewalls, antivirus, endpoint protection, etc.) 3
Perform regular cybersecurity assessments 3
Create and test an Incident Response Plan 4

3. Define a Data Backup & Recovery Strategy 4

Identify critical systems and data repositories 4
Choose the right backup architecture (cloud, on-prem, hybrid) 4
Test backups regularly to validate recovery 4
Ensure encryption and compliance for stored data 4

4. Rebuild a Business Continuity & Disaster Recovery (BC/DR) Plan 4-5

Perform a Business Impact Analysis (BIA) 4
Conduct a risk assessment 4
Develop actionable BC/DR playbooks 4
Test and update plans regularly through tabletop exercises 5

5. Align IT Strategy with Business Goals 5

Define a multi-year IT strategy that aligns with leadership priorities 5

Build an IT budget plan including investments in infrastructure, cloud, and cybersecurity 5

Identify opportunities for digital transformation and automation 5

Evaluate the need for a Fractional CIO to provide executive oversight 5

6. Optimize Vendor Management.....5-6

Create a full inventory of current IT and SaaS vendors 5

Review contracts and SLAs for cost and performance 5

Consolidate redundant services 5

Establish a centralized point of accountability for vendor issues 6

7. Plan for Ongoing Management & Support 6

Set up 24/7 infrastructure monitoring and support 6

Define patching updates, and maintenance schedules.....6

Establish clear escalation paths for incidents.....6

Identify support models (internal IT, co-managed, or MSP) 6

SMB IT Planning Checklist

This detailed checklist is designed to help small and mid-sized businesses (SMBs) build an IT foundation that supports growth, resilience, and operational efficiency. It includes expanded guidance on how to evaluate, plan, and execute key IT initiatives across infrastructure, security, continuity, and vendor management.

1. Assess Your Current IT Infrastructure

☐ Conduct a comprehensive IT Infrastructure Assessment

Assess your entire technology stack — from networks and servers to endpoints and storage — to identify weaknesses, performance issues, and security risks. Document all systems and map dependencies to create a clear baseline.

☐ Identify scalability challenges and bottlenecks

Look for aging equipment, outdated software, or network congestion that could prevent your business from growing efficiently. Plan upgrades based on growth projections.

☐ Benchmark your systems against industry standards

Compare your environment to best practices and compliance frameworks like NIST, CMMC, HIPAA, or ISO to uncover gaps and prioritize fixes.

☐ Assess alignment with compliance frameworks (e.g., HIPAA, CMMC, NIST)

Ensure your infrastructure meets regulatory standards if you're in a compliance-heavy industry like healthcare or finance.

Tip: Consider a third-party infrastructure audit to uncover hidden risks and inefficiencies.

---

2. Strengthen Cybersecurity Posture

☐ Establish a cybersecurity framework tailored to your business

Define clear policies and procedures for protecting your systems, including access controls, password policies, and acceptable use policies.

☐ Deploy and maintain security tools (firewalls, antivirus, endpoint protection, etc.)

Use layered security tools and ensure they're configured correctly and kept up to date to protect against malware, ransomware, and intrusion attempts.

☐ Perform regular cybersecurity assessments

Conduct vulnerability scans and penetration testing to identify and fix exploitable weaknesses in your systems and applications.

☐ **Create and test an Incident Response Plan**

Have a written, practiced plan that outlines how your team will respond to a cyberattack or data breach, including roles, timelines, and communication strategies.

Tip: Fractional CISO services can provide strategic cybersecurity leadership without the full-time cost.

---

3. Define a Data Backup & Recovery Strategy

☐ **Identify critical systems and data repositories**

Determine which systems and datasets are mission-critical for your operations and prioritize them for backup and recovery.

☐ **Choose the right backup architecture (cloud, on-prem, hybrid)**

Select a solution that matches your recovery objectives (RTO/RPO), security needs, and budget. Consider geographic redundancy for added protection.

☐ **Test backups regularly to validate recovery**

A backup is only useful if it works. Regularly perform test restores to verify data integrity and recovery time.

☐ **Ensure encryption and compliance for stored data**

Encrypt data at rest and in transit, and ensure your backups meet regulatory standards for data protection.

Tip: Integrate disaster recovery with business continuity planning to ensure a fast return to normal.

---

4. Build a Business Continuity & Disaster Recovery (BC/DR) Plan

☐ **Perform a Business Impact Analysis (BIA)**

Identify the financial and operational impact of downtime on each business function and prioritize recovery strategies accordingly.

☐ **Conduct a risk assessment**

Evaluate potential threats (cyberattacks, natural disasters, system failures) and determine your level of exposure and tolerance.

☐ **Develop actionable BC/DR playbooks**

Create role-based response plans for business continuity and disaster recovery. Include communications, logistics, and technical recovery steps.

☐ **Test and update plans regularly through tabletop exercises**

Simulate real-world incidents to test your team's readiness and improve response times. Update plans after each test.

Tip: Partnering with a provider like Balancelogic ensures you have 24/7 support and a tested recovery model.

---

5. Align IT Strategy with Business Goals

☐ **Define a multi-year IT strategy that aligns with leadership priorities**

Build a roadmap that aligns IT goals with business objectives, factoring in growth, innovation, and operational improvements.

☐ **Build an IT budget plan including investments in infrastructure, cloud, and cybersecurity**

Forecast costs and plan investments that offer the greatest return on business enablement and risk reduction.

☐ **Identify opportunities for digital transformation and automation**

Look for ways to use technology to streamline operations, improve customer experience, and reduce manual work.

☐ **Evaluate the need for a Fractional CIO to provide executive oversight**

Consider bringing in an experienced IT leader on a part-time basis to guide strategy, manage vendors, and oversee large initiatives.

Tip: Strategic IT planning reduces costs, enhances agility, and gives you a competitive edge.

---

6. Optimize Vendor Management

☐ **Create a full inventory of current IT and SaaS vendors**

Document all technology partners, contracts, services provided, renewal dates, and support contacts.

☐ **Review contracts and SLAs for cost and performance**

Ensure each vendor is delivering what they promised. Renegotiate contracts where costs are too high or service is lacking.

☐ **Consolidate redundant services**

Eliminate overlapping tools and platforms to reduce costs and complexity.

☐ **Establish a centralized point of accountability for vendor issues**

Assign one person or provider to manage all vendor relationships and serve as the escalation point.

Tip: Expert vendor management can reduce tech costs by 20-30% annually.

---

7. Plan for Ongoing Management & Support

☐ **Set up 24/7 infrastructure monitoring and support**

Ensure systems are monitored around the clock for outages or security incidents to minimize disruption.

☐ **Define patching, updates, and maintenance schedules**

Keep systems up to date to avoid vulnerabilities and performance issues. Schedule regular maintenance windows.

☐ **Establish clear escalation paths for incidents**

Make sure your team knows who to call and what steps to follow when a system fails or a threat is detected.

☐ **Identify support models (internal IT, co-managed, or MSP)**

Choose the right mix of in-house and outsourced support based on your team size, budget, and technical complexity.

Tip: Managed IT Services, like ITAssurance, offer proactive support, reduced downtime, and predictable costs.

If you have any questions, feel free to contact Bill Campbell at

bcampbell@balancelogic.com or (301) 396-8455.

Like us on Facebook
facebook.com/Balancelogic

Follow us on LinkedIn
linkedin.com/company/balancelogic-llc

Follow us on Twitter
@balancelogic

Subscribe to our YouTube channel
youtube.com/balancelogic

Learn more about us on our website.

https://balancelogic.com

About Us

Balancelogic is in its 21st year as a leading, Veteran owned business solutions and services company. At Balancelogic, we empower small and mid-sized businesses with enterprise-grade technology strategy, leadership, and execution — without the enterprise price tag. From IT strategy and cybersecurity to cloud, infrastructure, and automation, we deliver scalable solutions tailored for growth, resilience, and performance. Our team acts as an extension of yours, offering fractional leadership, hands-on support, and results-driven innovation that aligns with your business goals.

Let's build a smarter, more secure, and future-ready organization — together.
