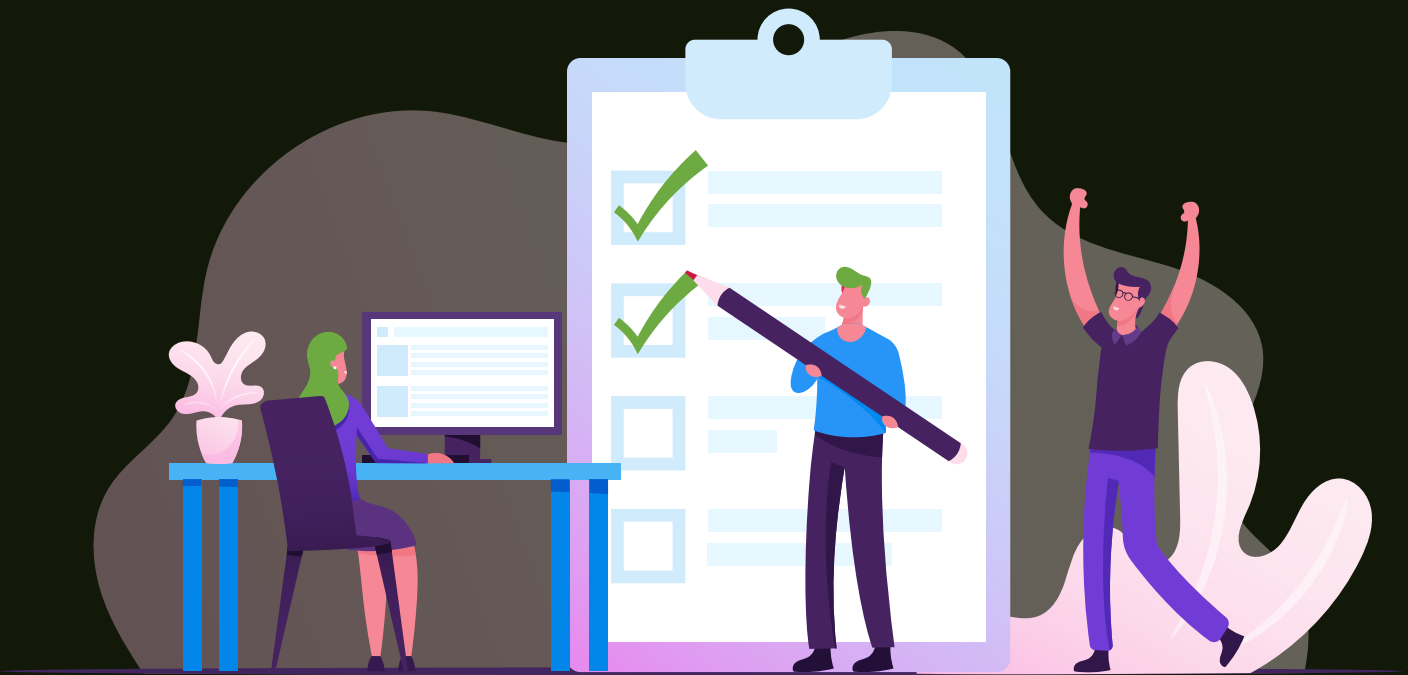


A FUNDAMENTAL IT CHECKLIST FOR SMALL BUSINESSES



A FUNDAMENTAL IT CHECKLIST FOR SMALL BUSINESSES

TABLE OF CONTENTS

What are the IT difficulties of small businesses today?	1
The objectives of this IT checklist	2
IT checklist for small businesses	3
1. Planning your IT adoption journey	
2. Building your infrastructure	
3. Managing your IT system	
4. Running your IT infrastructure	
Glossary of unfamiliar terms	11

What are the IT difficulties of small businesses today?

Technology is a nonnegotiable factor in the success of small businesses today. Not only has it become critical to operational efficiency, but also to client communication. New innovations have allowed organizations to significantly boost their productivity and revenue, and stay ahead of the competition.

For instance, online collaboration tools like Zoom and Microsoft Teams allow employees to collaborate remotely. Meanwhile, customer relationship management (CRM) software like Salesforce and Microsoft Dynamics 365 have made it easier for businesses to know clients better to increase customer satisfaction.

Despite this, there are many challenges that small businesses are facing today, such as:

#1 Lack of an in-house IT team

Small businesses typically do not have an in-house IT department because they have a limited budget that they'd rather use on important business processes. While this may not be a problem for some small businesses in the short term, it can be detrimental over time.

For instance, when an operating system (OS) such as Windows reaches its end of life, an organization's computers will no longer receive updates. Without a proper IT team, small businesses may find it difficult to upgrade their systems to a more modern OS. An organization may also take more time to recover from disasters.

#2 Security risks

The cyberthreat landscape is becoming more dangerous. Before, malware only inflicted damage on actual machines, but the rise of [ransomware and cryptojacking](#) is posing new security challenges to small businesses. Cybercriminals are even [taking advantage of the recent coronavirus pandemic](#) to steal data for their own gain.

Unfortunately, many small businesses falsely believe that they are not the target of these threats. According to a recent report by the [Ponemon Institute](#), 67% of companies with fewer than 1,000 employees have become victims of a cyberattack, while 58% have experienced a data breach. This is because cybercriminals are taking advantage of the weak cybersecurity protocols of small businesses.

#3 Absence of an IT strategic plan

To thrive in their industry, businesses must not waste time and resources on opportunities that may not be aligned with their long-term objectives. An IT strategic plan will serve as the ultimate guide to stay on track toward achieving business goals.

However, many small businesses lack an IT strategic plan, either because they believe that it is only for larger enterprises or that it's not a priority compared to other business concerns. But what they fail to understand is that without a strategic plan, they lack the direction they need to survive and succeed.

The objectives of this IT checklist

Many factors come into play when small businesses adopt IT. Many think of dealing with technology as a never-ending task that becomes more difficult over time. But if businesses take things slowly and carefully, they are more likely to succeed at integrating technology into their business.

This IT checklist provides a list of action items that guides businesses on how they can properly utilize and manage their IT infrastructure. It is divided into four activities that businesses have to perform:

- 1. Planning your IT adoption journey**
- 2. Building your infrastructure**
- 3. Managing your IT system**
- 4. Running your IT infrastructure**

In case you encounter some unfamiliar terms, a glossary is available at the end of this eBook.

At the end of this checklist, your business should be able to:

- Define your organization's IT direction and how it affects your business goals and objectives
- Deploy, install, and maintain hardware and software equipment
- Regularly review IT needs and legal requirements
- Have a comprehensive backup and cybersecurity plan in case of disasters such as cyberattacks, insider attacks, power outages, and pandemics, among others
- Have an access control policy that limits who can view, modify, and delete certain files
- Train new users on how to use your hardware and software
- Troubleshoot faulty machines and connections, and clean malware-infected computers



IT checklist for small businesses

1. Planning your IT adoption journey

Setting a general direction

Before you start planning your IT, think of where you want to go and what you need to accomplish for both the short and long term.

- You have an idea of why your business needs IT. For instance, IT can boost your office productivity and get things done faster than before. Or, you can use it to communicate with clients and partners remotely.
- You have identified the technology that your business currently needs and will need in the future. This could be storage systems, software applications, or new hardware.
- A sufficient budget to procure technology and replace outdated systems is in place.

Mitigating IT risks

No business will be able to adopt IT without running into risks and other issues. Make sure that you have identified all the obstacles that you might encounter and planned how your business will deal with them.

- You have an idea of how long your business can survive without IT. This could be around one day, one week, or one month.
- All the issues you might encounter have been listed down, including their causes and consequences. For example, without an internet connection, you won't be able to send files to your partners and connect with your clients.
- You have identified all the industry compliance risks. For example, since the Health Insurance Portability and Accountability Act (HIPAA) requires businesses to protect patients' medical records and other health information, it's understood that your business could be fined or shut down for not following protocol.

2. Building your infrastructure

Installing new equipment and drivers

When buying new equipment, purchase the essentials first and avoid the impulse to buy unnecessary items.

- The hardware and software you have purchased is suited for business environments. For example, home versions of operating systems (OS) like Windows 10 are meant for only one user, compared to multiple copies with the Enterprise variant.
 - The equipment comes with a warranty contract. This can ease the problems you may encounter in the future. If one of your computers suddenly malfunctions, its warranty contract can cover the repair costs.
 - You purchase equipment by brands and manufacturers you're already familiar with. Sticking with one manufacturer for your desktop computers (e.g., HP, Dell, or Lenovo), for instance, would ensure better compatibility. This also saves you the trouble of going into different service centers in case they need to be repaired.
 - The appropriate drivers for your equipment have been installed. When you first connect your printer to your PC, for instance, it will need to install drivers to communicate with your system properly.
-

Deploying software and security patches

After procuring your hardware, you must carefully deploy the appropriate software and patches to ensure compliance with license agreements and hardware compatibility.

- You have an in-house IT professional who will be responsible for deploying your software and security patches. If you don't have one, you must establish a working relationship with a trustworthy third-party professional like a managed IT services provider (MSP) such as RBS.
- You have a list of licensed software to be installed on your computers. Those that are not on the list must be removed from your computer.

- There is a designated person to handle downloading, verification, and deployment of patches.
- The designated person has decided on a deployment policy for software patches. They could install updates immediately or test them first on your systems before launching them.

Maintaining records of licenses and contracts

Once you deploy your software, it can be difficult to keep track of them. Your software programs typically come with a license, and it's important to know where they are installed so you can renew or remove them accordingly.

- Someone is keeping a list of what software applications are installed on every machine, along with their respective license agreements.
- You also have someone to keep a list of your domain names and web hosting arrangements. They are responsible for reminding you to renew these licenses and contracts.

3. Managing your IT system

Regularly reviewing your IT

The IT needs of your business will always evolve. Have an in-house expert or an MSP regularly check if your hardware is still helping you meet your goals.

- You regularly check and replace out-of-warranty equipment, if needed.
- You regularly discuss your IT needs with an IT expert.
- You constantly review if your IT service provider is still helping your business grow. In case they aren't, you have someone you can report issues to.

Meeting legal requirements

Your business must follow laws to avoid incurring fines and other penalties.

- Your business is following the necessary data privacy laws. Organizations in California must comply with the [California Consumer Privacy Act \(CCPA\)](#), which requires businesses to disclose their data collection and sharing practices to consumers. The EU's [General Data Protection Regulation \(GDPR\)](#), meanwhile, establishes rules on how companies can process the personal data of EU citizens and other entities.
- Someone is responsible for regularly checking if your business is still complying with applicable laws and regulations.
- If you are having difficulty complying with legal requirements, you are able to consult a specialist who can check your compliance requirements.

4. Running your IT infrastructure

Recovering from disasters such as fires, flood, accidents, and cybercrime

There are many disasters that can affect your business, so be prepared in case one causes downtime.

- You constantly review if your IT service provider is still helping your business grow. In case they aren't, you have someone you can report issues to.
- You have a step-by-step disaster recovery plan for your company to follow. You have also ensured that employees know where to access it.
- You have tested your disaster recovery plan with employees at least once or twice within a specific period so company personnel are prepared in case of any eventuality.



Maintaining data access rules

Your business needs to control who can access certain data to prevent intruders from stealing or destroying them.

- There are written rules on who is allowed to access, modify, and delete certain data. That means only department managers are allowed to see confidential data to prevent other employees from mistakenly or intentionally altering or deleting it.
- You have assigned one or two persons to add new users to your network and revoke their access when they resign or are terminated from your company.

Creating and resetting passwords

To ensure maximum data security, you need to control how your employees create and reset passwords.

- Users can change their passwords when they need to. This process should include a verification system to prevent cybercriminals from posing as an employee.
- Your IT system has a policy that locks a user out after three failed login attempts.
- A network administrator can reset the password of someone locked out. In case they are away, an assistant or a backup person could cover for them.
- Your IT policy should require users to reset their passwords after a certain period (every month or every three months, depending on your situation).
- You have password creation policies that indicate password length and characters to be used (alphanumeric, with symbols, etc.)

Training employees to use hardware and software

Your employees will experience a learning curve when doing their assigned tasks. By constantly training them, you help them do their job faster.

- You have identified your employees' tasks and the equipment they need to perform such tasks.

- You have trained them to ensure that they are able to perform their tasks efficiently.
 - You check on the progress of your employees' tasks.
-

Making and restoring from backups

There will be situations where you lose your business's data. Taking a proactive approach lets you immediately recover your files.

- You have a step-by-step backup process and have assigned someone to back up servers every day. They should be able to identify and respond to issues regularly. Another person must cover for them should they be unavailable.
 - You have a documented restore process and you regularly test if you can restore data from backups.
 - Some of your backups are stored off-site to prevent all of your data from becoming inaccessible should one backup become unavailable, corrupted, or compromised.
 - Crucial files are backed up on your server and not on a user's local drive.
-

Setting up and maintaining the internet connection

A good internet connection is important for businesses in the daily conduct of operations and for collaboration, among other uses.

- All ideal internet service providers (ISPs) have been thoroughly vetted. Factors such as offered speeds, data caps, and price should be considered.
- A "network administrator" is assigned to manage the technical aspects of connecting your computers to the internet. If you experience a network outage, the network administrator will be the one to identify the problem and work with the ISP to restore the connection.

Managing servers

Servers are an important aspect of any business as they provide reliability, security, and data accessibility. Small businesses might want to set up a server to manage their intranet, mail, and files through servers, but not a lot of organizations have an in-house expert who can manage them.

- You must have good database administration policies in place. To do this, write the necessary steps with an expert server administrator.
- You know how to manage your servers in-house and when to call in an expert or a service provider.
- You have a good relationship with an expert or MSP familiar with your business and server setup. They must be available at a short notice to solve your server problems.



A FUNDAMENTAL IT CHECKLIST FOR SMALL BUSINESSES



How RBS can help you build your IT

By leveraging technology properly, your small business becomes more competitive with large enterprises. And when you need help ticking some items off this checklist, RBS can help. We will be with you every step of the way, from procuring the necessary equipment and setting up and maintaining your hardware to ensuring legal compliance and reviewing your business goals regularly. No matter your IT problem, we can help you design an IT system that brings your business closer to its goals

**Ready to adopt IT for your small business? Contact us today so we
can get right down to business.**

Phone: **(316) 425-0075** Email: **jay@ribbitbusiness.com**



WWW.RBSITSOLUTIONS.COM

Glossary of unfamiliar terms

Cloud computing – This involves the use of a network of internet-hosted remote servers to store, manage, and process information.

Cold site – This is a disaster recovery service that provides office space but requires the business to provide and install the necessary equipment to continue its operations.

Customer relationship management (CRM) software – CRM software is used to track all the collected client information, such as purchase history and product preferences. It is used to grow relationships with customers to improve future deals.

Domain name – A domain name is a unique name that identifies a website, such as “google.com” or “microsoft.com”.

HIPAA – HIPAA, or the Health Insurance Portability and Accountability Act, is designed to provide privacy standards to protect patients’ medical records and other health information provided to doctors, hospitals, and other healthcare providers.

Hot site – This is a disaster recovery service that provides fully equipped office facilities immediately available for businesses to continue critical operations.

Managed IT services provider (MSP) – An MSP is a firm that delivers managed IT services to clients under a subscription model. MSPs can monitor a business’s IT infrastructure round-the-clock for any threats that may harm the system. They can also help organizations adopt various technologies like cloud computing and Voice over Internet Protocol (VoIP), and more.

Network administrator – This person is in charge of maintaining an organization’s IT infrastructure. They install, organize, and support computer systems and networks.

Security patch – Also known as a hotfix or software patch, security patches are small programs that fix a security vulnerability in an application. It is important to install them immediately to prevent cybercriminals from exploiting security holes in programs.

Server – A server is a computer or system that provides resources, data, or programs to computers on a network.

Voice over Internet Protocol (VoIP) – VoIP is a service that enables internet-based voice communications without a phone line. It can also be used for video chatting and conferencing.

Warm site – Warm sites, compared to cold and hot sites, are partially equipped with necessary office items such as computers, telephones, and power supplies. They may not have all the facilities that the disaster-stricken business originally has.

Warranty – This is a written guarantee issued by a manufacturer that promises to repair or replace an item within a certain period without charging the buyer.

Web hosting – This is a type of internet service that allows individuals and businesses to make their website accessible on the World Wide Web (WWW).