VON JACKSON

THE 8 BASIC IT QUESTIONS

ALL COMPANIES SHOULD KNOW

FOREWORD

Welcome,

As a business owner or IT decision maker, you have a lot on your plate. But there's one important task that could save you time, money, and headaches down the line: documenting your technology stack.

In today's fast-paced digital world, businesses rely heavily on technology to operate efficiently and compete in the marketplace. However, many businesses struggle to keep track of the technologies they use, which can lead to a range of problems such as inefficiencies, security risks, and wasted resources. Without a clear understanding of their technology stack, businesses may be using outdated or unnecessary tools, spending money on software licenses they don't need, or leaving themselves vulnerable to cyber threats. By documenting their operational technologies, businesses gain greater visibility into their IT infrastructure, identify areas for improvement, and make more informed decisions about their technology investments.

In this e-book, we'll walk you through the process and give you tips to get started. Without further ado, let's discuss *"The 8 Basic IT Questions All Companies Should Know"*.

Best Wishes,

Von Jackson
Co-Founder of Marcoby
"At Marcoby, You're Technically Family"

WHY IS DOCUMENTATION IMPORTANT?

A study by Coveo found that the average employee spends 45% of their day searching for information. Interestingly, the average IT professional spends over 50% of their day looking for information. As businesses look to improve productivity and proficiency, a top priority should be documentation.

IT documentation is any and all recorded information relating to your IT environment, such as hardware devices, software tools, system requirements, design decisions, architecture descriptions, processes, and incident responses. It helps your organization understand how your IT systems work, how they interact with other components, and how to troubleshoot any issues and improve performance.

IT infrastructure documentation can bring many benefits to your business, such as:

Saving time and money
By documenting your IT infrastructure, you reduce the amount of time and resources spent on searching for information, resolving problems, and training new staff. With proper documentation, you can dramatically reduce wasted and boost your productivity and efficiency.

WHY IS DOCUMENTATION IMPORTANT?

Enhancing quality and consistency
By leveraging IT documentation , you ensure that your IT services are delivered in a standardized, reliable, and auditable way, regardless of who is performing them. You can also follow best practices to align operations with industry standards, such as ITIL (Information Technology Infrastructure Library), a framework of best practices for managing IT services and improving IT support and service levels.

Improving security and resilience
By defining organizational IT standards, you can protect your IT systems from cyberattacks and minimize the impact of incidents. It allows you to identify potential vulnerabilities and risks in your IT environment, implement preventive measures and security controls, and respond quickly and effectively when a breach occurs.

IT infrastructure documentation is not a one-time task, but an ongoing process that requires regular updates and maintenance. As your business grows and changes, so does your IT environment. You need to document any changes or additions to your IT infrastructure, such as new hardware devices, software updates, configuration changes, or process improvements. You should also review your documentation periodically and ensure that it is accurate, complete, relevant, and accessible.

IT documentation is not a luxury, but a necessity for any business that relies on technology. When properly developed, you gain a competitive edge in the market through enhanced efficiency, improved customer satisfaction with reduced downtime, and make better informed decisions to achieve your business goals.

DO YOU HAVE A NETWORK DIAGRAM?

Imagine this: your company's network goes down unexpectedly, and you're left scrambling to figure out what's causing the issue. You have no idea where devices are connected, how they're interacting with each other, or where the problem might be originating from. This is where network diagrams come in.

What Is IT?
A network diagram shows the physical and logical layout of the network devices, servers, routers, switches, firewalls, and other IT components.

Why should I know this?
The goal of a network diagram is to illustrate how digital information flows through the network. It is especially useful when:

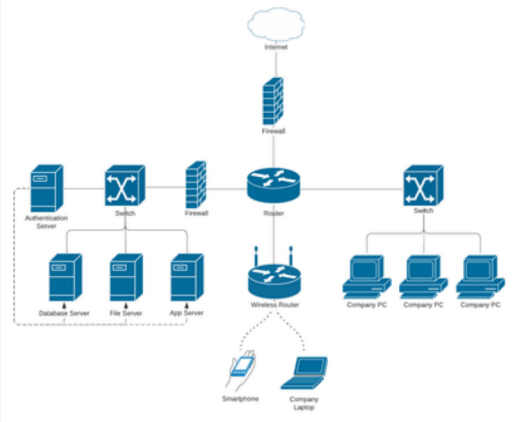
- Troubleshooting network issues - Helps to identify the devices and applications that could be contributing to the issue to.
- Resource Planning - When planning an IT budget, a network diagram can identify what could be affected by proposed changes or reveal opportunities to improve network design.
- Identify Potential Risks - The first step to securing any network is knowing what hardware and software exist on the network. In IT Security, this is commonly referred to a your "Attack Surface Area".

DO YOU HAVE A NETWORK DIAGRAM?

How Do I Get One?

Typically, a network diagram is created by using a diagraming tool. Some common software used are Microsoft Visio, Dia, Lucidchart, or Draw.io. Of course, if you don't have a tool, you can always draw one by hand. Keep in mind that as new devices are introduced and old devices are retired, the diagram also becomes invalid.

It is a best practice to review and update your diagram routinely for accuracy and completeness. There are many formats and templates for developing a network diagram. There are also different kinds of network diagrams, each with their own purpose. A LAN Diagram (pictured below) can illustrate a network at a single site. A Wide Area Network (WAN) diagram can be used to document how several sites are connected. Regardless of the type of diagram, the goal is always the same: How does digital information travel at my business?



An Example of a Local Area Network (LAN) Diagram

DO YOU HAVE A HARDWARE INVENTORY LIST?

How many devices are currently connected to your network? Who has them? Are they still supported? If you don't know these answers, it might be time to develop a hardware inventory list. Let's look at the benefits and a method for managing your hardware assets.

What is it?
A hardware inventory list is precisely as it sounds. It is an organized list of your hardware assets.

Why should I know this?
To effectively manage your hardware assets, a detailed list is needed to capture and maintain the information. A good list should be as detailed as possible, and a minimum should contain:

- Device Name
- Make and Model
- Device Class
- Serial Number
- Asset Number
- Purchase Date
- Purchase Cost
- End of Support Date
- Location
- Operating System
- Assigned User
- IP Address
- Any additional notes

Having this information available helps you answer all of the opening questions and more.

DO YOU HAVE A HARDWARE INVENTORY LIST?

How do I get one?

A hardware inventory list can be as simple as a word document or excel spreadsheet. For improved accuracy and efficiency, many organizations leverage IT asset management software to discover and document devices connected to the network. Some examples are ManageEngine Service Desk Plus, Auvik, Kaseya IT Glue, Jira Service Management, or Rippling. The biggest benefit of software is that the documentation process can be automated, improving accuracy and data consistency.

DO YOU HAVE A SOFTWARE INVENTORY LIST?

Do you know what software is lurking on your company computers? Are there applications no longer used still installed in your network? A software inventory list is the key to keeping track of your business applications.

What is it?
Similar to a hardware inventory, a software inventory list is an organized list of the applications used by your organization.

Why should I know this?
A major key to making your IT more predictable and manageable is reducing variance. This is known as "Standardization". A software inventory list plays a pivotal role in achieving standards for a company. It helps track license and subscription of software products used by the company. A software list can also help a business identify any redundant, outdated, or unauthorized software that may pose security or compliance risks. Additionally, a software inventory list allows a business to evaluate software usage and employee satisfaction which is useful in deciding on renewing or replacing the solution.

DO YOU HAVE A SOFTWARE INVENTORY LIST?

How do I get one?
Similar to the hardware list, a software list can be as simple as a document or produced using, well, software. A reliable list allows you to evaluate your defined standard vs what actually is installed on company devices. This list should include:

- Device Name
- Device Operating System
- Any installed applications
- Software licenses for installed applications
- Where the application installer is located
- How the application is administered
- Any additional notes

DO YOU HAVE AN IT SECURITY POLICY?

It is nearly impossible to run a modern business without the use of network-connected technologies. With this increased reliance on technology comes an increased risk of cyber-attacks and data breaches. That's where IT security policies come in.

What is it?
An IT security policy defines the roles and responsibilities of the IT staff, the access rights and permissions of the users, and the security measures and tools in place to protect your data and network. A policy is most often required by government and industry regulations. They are also required in many cyber insurance policies.

Why should I know this?
An IT security policy outlines a company's strategy for protecting possibly it's most important asset: its data. With the increasing frequency (and success) of cyber-attacks, it becomes more important to have a plan for prevention. Having a policy (or policies) enables you to more easily identify opportunities to better prevent an attack and what your organization would do if an attack were successful. They also serve as a tool for validating your security protocols by routine auditing of your environment. Lucky for you, if you have the answer to the questions asked thus far, you should have a solid understanding of your environment and know what policies exist or are needed.

DO YOU HAVE AN IT SECURITY POLICY?

How do I get one?

An IT security policy typically take the form of a document. Some examples may be a technology acceptable use policy for company devices or an incident response plan. They include stated objectives like preventing unauthorized access and techniques for achieving policy objectives like an identity and permissions management system. In developing policies, IT professionals often look at established best practices and frameworks. A few examples are CIS Critical Security Controls, NIST, ISO 27001, or CMMC. The use of any chosen framework is the same: to leverage its best practices and guide the development of your IT security policy.

Infographic created by Superior Support Resources

DO YOU HAVE SYSTEM FOR BACKING UP YOUR COMPANY DATA?

Data loss can be devastating for any organization. With the increasing prevalence of system failures and human errors, it's more important than ever to have a reliable backup system in place. But what exactly is an IT backup system, and how can you get one?

What is it?

An IT backup system is a process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost. This typically involves creating copies, storing them in a secure location, and testing them regularly for quality assurance. A good backup system considers:

- Frequency-How often backups should occur. This should be based on a recovery point objective (RPO) which is the maximum amount of data that can be lost after a data recovery. Put another way, it is current the data in the backup must be before data loss will exceed what is acceptable to an organization.
- Backup type-A system backup is used to back up the operating system, files and system-specific useful/essential data. Some types of backup systems are file backup, disk imaging, and cloud backup.
- Backup location-The storage location used to save completed backups.

DO YOU HAVE SYSTEM FOR BACKING UP YOUR COMPANY DATA?

- Desired restore speed - How fast data should be recovered. This is influenced by a recovery time objective (RTO) which is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. RTO sets the expectation for how long it will take to restore normal business operations after a data loss event.

Why should I know this?

A backup system is one of those things that you would rather have and not need rather than need and not have. While people often relate backups only to system failures and cyber-attacks, a much more common use is in moments of human error where a file or folder is deleted or changed in an irreversible manner. Having reliable backups can help prevent data loss, minimize downtime, and comply with regulatory requirements. Backups are a key operational safeguard and a central element of any business continuity plan.

How do I get one?

A system backup can be completed using built in software such as Windows Backup or MacOS Time Machine. The main issue with this approach for businesses is that they are not centralized which makes management and validation more difficult. Instead, many businesses rely on backup software to automate and centralize their backup system. Some notable backup systems are Veeam Backup and Replication, Acronis Cyber Protect, or Datto Business Continuity Disaster Recover (BCDR). The backup software space is highly competitive with numerous products, making the ability to find and implement one that work for your requirements easy.

DO YOU HAVE SYSTEM FOR RECOVERING YOUR COMPANY DATA?

Have you ever experienced the sinking feeling of realizing that important data on your device has been lost or corrupted? This is why data recovery systems are essential for any organization. But how do you get started? Let's take a closer look at what a data recovery system is and how you can implement one for your own recovery strategy.

What is it?
A recovery system outlines the procedures and tools for restoring data from a data backup. It is used to recover corrupted, lost, or deleted data from a backup system.

Why should I know this?
A data recovery system goes hand-in-hand with a data backup system. A backup system is only useful if you have a way of recovering the data when needed. A recovery system is critical in data loss events such as a device or operating system failure, accidental deletion, cybersecurity attack, or environmental disaster. Without one, the data loss can result in loss of productivity, intellectual property, and time reproducing the data. Depending on the data lost, it can also mean loss of revenue or fines and litigation from compliance failures.

How do I get one?
Much like a backup system, a recovery system is built and managed by backup software. With the software backing up the data, it has the ability to restore the data to the original device or a new one if needed. It is the RPO and RTO from the recovery system that influences the backup system. Therefore, the two go hand-in-hand.

DO YOU HAVE SYSTEM FOR MAINTAINING YOUR IT ASSETS?

Maintaining your IT systems is crucial to sustaining an operations. But how do you create an effective IT maintenance system? Lets explore what an IT maintenance system is, why it's important, and how you can efficiently create one using software tools and templates.

What is it?

An IT maintenance system provides technical support personnel with the information needed to maintain IT systems. It defines the support environment, roles and responsibilities, maintenance activities, and monitoring methods. It may include activities such as updating systems, reviewing logs for errors or warnings, or removing inactive accounts or devices from your environment. There are different strategies for maintaining an environment but by most standards, the best approach is a preventative maintenance system.

Why should I know this?

A maintenance plan can help organizations to prevent system failures, improve performance, enhance security, and reduce costs. It can also help to ensure compliance with industry standards and regulations. This can also be especially important in resource planning and budgeting as you'll be able to better predict IT usage. By having a system for maintaining your IT assets, you make your operational technologies more reliable and reduce the likelihood of downtime or data loss.

DO YOU HAVE SYSTEM FOR MAINTAINING YOUR IT ASSETS?

How do I get one?

A maintenance system is merely a collection of tasks and assigned responsibilities. For enhanced productivity and scalability, it is best to leverage software tools to automate the activities. There are also numerous templates that can be used to customize a plan that best suits your organization. Any maintenance strategy should define:

- What systems are maintained
- What techniques or templates should be used
- Who is responsible for maintenance
- How often maintenance should occur
- What measurable standard validates a system is in good health
- What steps should be taken if a system is observed to not be in good health after maintenance
- Are there any special instructions that require a deviation from your normal maintenance plan

DO YOU HAVE YOUR EXTERNAL VENDORS AND SERVICE PROVIDERS DOCUMENTED?

Outsourcing IT infrastructure elements to external service providers is becoming increasingly common in organizations. This can fill gaps in skills and reduce costs. But how do you track your agreements and what providers are expected to actually do? Documenting your external vendors and service providers helps your organization get what it is paying for. Keep reading to learn why this is and how to create one.

What is it?

In any organization, certain elements of your IT infrastructure will be delegated to an external service provider. When an organization does enlist the services of an external provider, it is best to document relevant details of the engagement for reference. This documentation should include:

- Responsibility - Phone Service Provider, Internet Service Provider, Business Application Support, etc.
- Contact Information - Company name, phone number, assigned client representative,
- Account Information - Assigned Account Number, account pin, account secret passcodes.
- Service Level Agreement (SLA) - A documented legal agreement with the provider identifying responsibilities and expected level of service (Expected response time, support hours, etc.)
- Service Cost - Amount paid monthly or annually for services.
- Service Renewal Date - Date the agreement ends and would need to be renewed to extend services.
- Any additional notes you find relevant

DO YOU HAVE YOUR EXTERNAL VENDORS AND SERVICE PROVIDERS DOCUMENTED?

Why should I know this?
Documenting your external vendors ensures your organization understands the expectation of service from the provider. By having SLA and cost details, you have a means of analyzing the effectiveness of the resource and the value of the engagement. By having the renewal date, you ensure you avoid a lapse in service. By having a clear understanding that can be referenced, you improve organizational satisfaction and ability for informed analysis.

How do I get one?
An organization should keep this information in an easily accessible place. It's format is not as important as is having the information. Many organization use systems such as a CRM or digital documents like a document or spreadsheet that can be easily updated as needed.

A FAREWELL

Well my friend,

I hope you find this information useful. Here's a quick recap of the questions:

1. Do you have a network diagram?
2. Do you have a hardware inventory list?
3. Do you have a software inventory list?
4. Do you have an IT security policy?
5. Do you have system for backing up your company data?
6. Do you have a system for recovering your company data?
7. Do you have a system for maintaining your computers and network devices?
8. Do you have your external vendors and providers documented?

As you use these questions to assess your IT infrastructure and relevant documentation, I hope they bring more clarity and structure. If you decide you need help in developing this documentation and optimizing your IT infrastructure, Marcoby is available to assist.

Visit our website at marcoby.com or email us at learnmore@marcoby.com to get more information.

Best Wishes,

Von Jackson
Co-Founder of Marcoby
"*At Marcoby, You're Technically Family*"