



THE 3 ESSENTIAL TECH SYSTEMS YOU MUST HAVE IN PLACE TO GROW & PROTECT YOUR BUSINESS

A WORKBOOK FOR BUILDING YOUR IT ROADMAP ONE STEP AT A TIME

Does your business have an IT strategy in place? An “IT Roadmap?”

No doubt you hear this terminology regularly, but maybe you aren't sure how it applies to your small-business or organization.

This workbook is an opportunity to grade yourself and your business, and discover simple tactics and strategies you should be utilizing to protect your data and assets while plotting your path for future growth. Chances are, your organization has a heavy focus on tactical management of your IT resources and procedures, without an emphasis on the long-term goal setting needed to move forward. The tactics are primary and need to be firmly in place before an organization can move on to big-picture thinking and planning.

To really grow your business you need to manage your tactics *and* your strategy.

The 2 Styles of IT Management.

Strategic Technology Management

- ✓ Defining goals and requirements.
- ✓ Planning, preparing & measuring.
- ✓ Automation to lower & contain technology costs.
- ✓ Develop budgets and priorities.
- ✓ **CANNOT** be easily delegated or outsourced.

Tactical Technology Management

- ✓ Reacting to changes and events.
- ✓ Consists of the tactical execution of technical tasks or task lists, (responding to users requests for help, installing updates, virus removal, patching, tracking, reporting, monitoring, software license renewals, upgrades, updates, moves/adds/changes, log files, dealing with vendors such as ISPs, Copiers, Telephone vendors, line of business applications, domain renewals, SSL renewals, PCI compliance audits, software upgrades, equipment replacements, hardware/software purchases, warranty processing of equipment, troubleshooting software bugs, installing printers, drivers, scanners, setting up new cell phones, firewall upgrades, monitoring and changes, etc.)
- ✓ Can (and should be) outsourced or delegated.

Getting Started.

These are the basics.

Level 1 sets you up with security measures to protect your data with scheduled backups (image-based) as well as protective anti-virus/anti-spam software on all workstations and servers. You utilize a network firewall and maintain a system of password management for your team.

In addition, you have basic network monitoring performed on a regular basis, (with notifications as needed). You also have a team of IT support professionals on standby to assist with network, security and disaster recovery issues as they arise.

Level 1 is a tactical approach to your IT, with little in the way of long-term, strategic planning in the mix.

Level 1 Technology Fundamentals You MUST Have In Place

Item	True or False	Grade
You have data backups of ALL critical servers and workstations. You test the backups daily for corruption, loss or destruction. You resolve backup jobs daily. You conduct monthly scheduled test restores "fire drills" to ensure all data is backed up and able to be recovered BEFORE you need it.	True/False	
Your data backups are image based. You have both local and offsite backups. You could complete an entire system restore from the data backups in less than ½ day for any critical computer or server on your network.	True/False	
You have up-to-date antivirus and anti-spam software on all workstations and servers. You regularly apply updates and security patches and have an easy way to restore computers and servers should they become inoperable from a fatal virus infection.	True/False	
You have a firewall on the network that is tested regularly to ensure that there is no suspicious traffic. All of your wireless access points are secured (meaning they require a unique password for entry). This password is not publicly posted or shared with employees but is given on a need to know basis.	True/False	
Your entire organization uses complex passwords. Users do not share or post passwords. Only you and executive management have access to your administrator password to all servers, routers and firewalls. You have a defined process for allowing access to 3 rd party vendors to access your network via a guest account with a defined procedure to close their access immediately after work is completed.	True/False	
You have access to up-to-date network documentation including usernames, passwords, vendor support contract ID's, software licenses and key codes for all software, and a list of software expiration dates including SSL and domain renewals. You systematically update this information and keep a copy offsite in case of an emergency.	True/False	
You have basic network monitoring to ensure your systems are operating at optimal speed and performance. You are notified automatically when thresholds are not met.	True/False	
You have a team of IT professionals and automated systems on standby with skills ranging from end user support and network administration needs to security and disaster recovery. You do not rely on a single person to manage or update your systems.	True/False	

What's Next?

Level 2 incorporates all elements of Level 1, but utilizes a more systematic, proactive approach towards IT issues and initiatives.

Level 2 begins to incorporate a strategic overview to your IT management, utilizing IT automation and planning tools. At this level you are adding more protection and efficiency to your technology systems and procedures.

Backup Internet service may be used as a fail-safe option, and a well-documented Business Continuity/Disaster Recovery plan is written and tested on a regular basis.

At Level 2 you are utilizing a portal that monitors all systems with alerts that allow you to track and spot issues and problems. Your stand-by support team assists with this maintenance and is available when needed.

Level 2 Technology Fundamentals You MUST Have In Place

Item	True or False	Grade
<p>You have a systematic, proactive approach and operating procedure for all of the following:</p> <ul style="list-style-type: none"> • Data backups and recovery of files. • Offsite data protection and the ability to virtualize data & systems for access. • Breaches to security, logging reporting and security response via a managed firewall or Unified Threat Management system. • Spam, spyware, malware and virus protection against unauthorized access to network. • End user support. • Ability to perform changes to the network such as addition of users, printers, devices or new email accounts. • Hardware or software failures for servers, routers, switches, printers, computers, laptops and tablets. • Identifying and applying critical updates and security updates to hardware, software and network equipment. 	True/False	
<p>You have an automated and centralized way to prevent, detect and remove viruses and spam. When security thresholds are approached, you have automated tools and services that notify your network administrate or IT team for investigation and remediation to problems.</p>	True/False	
<p>You have multiple internet service providers which act as fail-overs so that if one goes down your entire organization can continue to connect to the internet. You have the ability to limit and prioritize internet traffic based on business priority and sensitivity.</p>	True/False	
<p>You have a well-documented disaster recovery plan that is tested on a routine basis. You are 100% confident that your company's critical data and the systems could be recovered in a reasonable time frame for their required function. You know how long your business can afford to be down (in terms of time and money) BEFORE you execute your disaster recovery plan. You have calculated and know how much one hour or complete downtime costs.</p>	True/False	
<p>You know what your IT Support will cost each month and have a budget for hardware, software, and services defined and allocated. You review this plan at least annually with your IT provider or CIO to make adjustments as needed.</p>	True/False	
<p>You have a portal where you can login to see what types of issues end users are reporting, monitoring alerts, backup failure & success alerts so you can track trends and spot problems. You have a team and toolsets on stand-by that are available either during working hours or available for after hours support depending on your business requirements.</p>	True/False	

Maximizing Your IT

Level 3 is where real growth happens.

This is where the strategy comes in. At this level you have the basics down pat, with automated, secure IT systems in place. You have budgets, disaster plans and ops procedures that are documented and tested regularly. It's time to begin building a strategic, growth-oriented technology system that includes:

- A technology roadmap that outlines your business goals and priorities. A defined plan is in place to reach these goals and this document is updated regularly.
- An established process for reviewing productivity and cost issues.
- Access to a CIO level consultant to assist with planning your IT roadmap, offer guidance with network design, risk management, compliance issues and more.

Level 3 Technology Fundamentals You MUST Have In Place		
Item	True or False	Grade
You have a technology roadmap that is updated at least annually against desired business outcomes and your company's top priorities or quarterly goals. You identify at least 1 – 5 ways to improve your network or leverage your existing technology resources to save time, money or resources. You have a defined action plan to implement these goals.	True/False	
You review employee productivity issues and implement the following strategies to lower costs and improve productivity: <ul style="list-style-type: none"> • Internet acceptable use policy along with a system to enforce, track and monitor it • Multiple monitors • Automated anti-spam and anti-spyware • Equipment replacement strategies to increase performance and speed • Software licensing and licensing programs to reduce cash outflow • Review hardware, software, internet service provider contracts to negotiate better terms and pricing based on business needs 	True/False	
You measure and report trends such as security risks, bandwidth usage, employee activities, and network resource performance to identify problem areas. From there, you create strategies and systems to mitigate risk, lower costs, increase efficiency, and improve employee productivity.	True/False	
You measure and report trends such as security risks, bandwidth usage, employee activities, and network resource performance to identify problem areas. From there, you create strategies and systems to mitigate risk, lower costs, increase efficiency, and improve employee productivity.	True/False	
You have access to CIO Level Advisory Services as needed to explore new technologies, seek guidance on advances, and opportunities to drive business outcomes. You use technology as a tactic to achieve your company's quarterly and annual objectives. You avoid expensive mistakes because you have access to IT strategic resource planning and best practices.	True/False	
You complete an annual risk management review from a data and operations standpoint to ensure you have adequate systems, processes, people, resources and insurance to protect your company.	True/False	

Ready to take the next step?

Got your grade?

Let's talk about how eGuard Tech Services' knowledge and expertise can help you define, and achieve your technology goals.

Let's start a conversation.