IT Service Excellence Tool Kit

How to meet and exceed customer expectations to ensure customer retention

By Kevin Gibson and Vernon Southmayd
# Table of Contents

**Part I: Key Fundamentals and Best Practices for IT Service Delivery**

- What is a Service Desk and Why is it Important to Your TSP? .............................................. 6
- What is a Help Desk and Why is it Important to Your TSP? ........................................... 8
- What is a Help Desk and How is it Implemented? .............................................................. 8
- What Standards Should Be Implemented By a Best Practice Help Desk? ......................... 9
- A Help Desk Will Assist in Enabling a Client to Meet Their Strategic Goals ................. 9
- What Are the Critical Differences Between a Service Desk and a Help Desk? ................. 9
- A Help Desk Focuses on End-User Needs ........................................................................... 10
- A Service Desk Focuses on Client Strategy ....................................................................... 10
- A Help Desk is a Component of a Service Desk ............................................................... 11
- Many Companies Have a Help Desk Without a Service Desk ....................................... 11
- Few Companies Have a Service Desk Without a Help Desk ........................................... 11
- When Should You Use a Service Desk vs. a Help Desk or Do You Need Both? ............. 11
  - Help Desk is Technically Focused .................................................................................. 12
  - Service Desk is Customer and Process Focused ........................................................... 12
- Your Business Will Benefit the Most with Both a Service Desk and a Help Desk .......... 13
- Service Desk Manager ...................................................................................................... 15
- Roles and Responsibilities Within a Service Desk .......................................................... 15
  - Service Desk Supervisor/Senior Service Desk Analyst .................................................. 16
  - Service Desk Analyst or Technician ............................................................................. 17
- Incident Manager .............................................................................................................. 18
- Problem Manager ............................................................................................................ 18
- Change Manager ............................................................................................................ 18
- Release Manager ........................................................................................................... 18
- Configuration Manager ................................................................................................. 18
- Roles and Responsibilities Within a Help Desk .............................................................. 19
  - 1st Level Support ......................................................................................................... 19
  - 2nd Level Support ....................................................................................................... 19
  - 3rd Level Support ....................................................................................................... 19
- Support Considerations ................................................................................................. 20
- Service Deliverables. What Should a Help Desk and Service Desk Support? ................ 20
- Daily Activities ............................................................................................................... 22
- Help Desk Daily Duties ................................................................................................... 23
- Service Desk Daily Duties ............................................................................................... 24
- Service Agreements and SLAs ....................................................................................... 25
- Service Agreement Considerations ................................................................................ 26
- Services to Support SLAs ............................................................................................. 27
- Vendor Management Services ....................................................................................... 27
- The Value of Vendor Management ................................................................................ 27
- Reporting ....................................................................................................................... 28
  - The Value of Reporting ............................................................................................... 28
- Client Satisfaction .......................................................................................................... 30
  - What TO Say and NOT to Say ..................................................................................... 30
- Measuring Client Satisfaction ......................................................................................... 31
- Survey Customers .......................................................................................................... 31
- Understand Expectations ............................................................................................... 32
- Find Out Where You're Failing ....................................................................................... 32
- Pinpoint Specifics ........................................................................................................... 32
- Assess the Competition ................................................................................................. 32
- Retaining Clients ............................................................................................................ 33
  - Set Expectations .......................................................................................................... 33
  - Be the Expert ................................................................................................................ 34
  - Go the Extra Mile ......................................................................................................... 34
- Measuring Performance .................................................................................................. 35
  - KPIs .............................................................................................................................. 36
- Processes Within Service Delivery .................................................................................. 38
  - Incident Management ................................................................................................ 38
  - Problem Management ................................................................................................. 38
  - Identification and Classification of Problems ............................................................... 39
  - Problem Tracking and Resolution ............................................................................... 39
  - Problem Closure ......................................................................................................... 39
  - Change Management .................................................................................................. 39
  - Risk Management ....................................................................................................... 41
- Clients ................................................................................................................................ 43
  - Client Qualifications for Service ................................................................................ 43
  - Setting Minimum Client Qualifications for Service .................................................... 44
  - Setting Minimum Infrastructure Qualifications for Service ....................................... 46
- Hardware and Hardware Devices .................................................................................. 47
- Operating Systems and Applications Software .............................................................. 47
- Connectivity Requirements ............................................................................................ 48
KEY FUNDAMENTALS AND BEST PRACTICES FOR IT SERVICE DELIVERY

PART 1
What is a Service Desk and Why is it Important to Your TSP?

A service desk understands that information offers technology solution providers (TSPs) strategic advantages and ensures proper mechanisms are in place for the data to be analyzed, produced and distributed seamlessly. The best service desks manage information delivery by utilizing Information Technology Infrastructure Library (ITIL) best practices to deliver these services.

According to the ITIL, a service desk is the single point of contact between users and IT service management. Tasks include handling incidents and requests, and providing an interface for other ITIL processes. The primary functions of the service desk are incident control, life cycle management of all service requests, and communicating with the customer.

Another definition of service desk is a center that provides a single point of contact between a company’s customers, employees and business partners. The service desk is designed to optimize services on behalf of the business and oversee IT functions. Thus, a service desk does more than ensure IT services are being delivered at that moment; it manages the various lifecycles of software packages used to provide critical information flow by utilizing ITIL best practices.

These best practices enable a technology solution provider to ensure end-user data is being delivered consistently under many different scenarios. Since the service desk is a single point of contact (SPOC), it understands that there are many reasons services can be interrupted. A service desk has the means within its hierarchy to monitor and manage each layer of service from beginning to end. These layers are classified by:

- **Network Operations:** The ability to monitor all network devices and connections remotely. A service desk manages and monitors incident reports, traffic, performs network reviews, implements backups and manages
change on the network. Thus, a service desk ensures the infrastructure of the network is optimized to meet the business needs of the enterprise.

**Systems Operations:** The ability to perform core systems management tasks. Core systems management includes performance monitoring, installation of patches, change management, account management and support for specific platforms, Windows, Linux, Mac, etc.

**Database Operations:** The ability to maintain and optimize database tasks. Performance monitoring, fault monitoring, log reviews, access management, and change control for database software such as Microsoft SQL, Oracle, MYSQL, etc.

**Security Management:** The ability to protect the enterprise from external/internal threats. A service desk will perform vulnerability scans, monitor IPS logs and map this data to the information security related regulatory mandates.

All of the functions described above are delivered by utilizing various types of hardware, software and delivery processes. All of these functions have to work together in a seamless manner and each has its own lifecycle, and the service desk will manage them. Thus, when one hardware platform, software package or process needs to be replaced with newer technology or practices, the service desk will manage the transitions ensuring maximum data delivery.

By performing the tasks outlined above, a service desk improves user satisfaction by:

- Minimizing business impacts of service failures
- Proactively managing use of the IT network of ITIL best practices
- Resolving incidents and requests with minimal delay
- Communicating with the end-user

As technology solution providers switch their IT service management from technology based to process based, they are able to integrate their IT practices directly into the client’s overall strategic and business plan. The service desk plays a strategic role in this transition. The service desk allows clients to be less dependent on specific technology and enables them to easily connect with business partners moving forward by focusing on processes. By switching the IT focus on processes, the infrastructure delivers value add to the client’s users and customers. Once the services and processes are defined, the service desk monitors them and the client focuses on its strategic and tactical business plan.

A good service desk improves a client’s customer satisfaction by allowing the client to implement their business plan without having to be troubled with technology needs. A good service desk improves a client’s satisfaction by managing IT costs while managing the lifecycles of the IT processes and by utilizing ITIL best practices. A good service desk communicates effectively and efficiently with each end-user. There are many more things a good service desk does well; it is the next step in allowing your business to help your client to focus specifically on their business plan.
The key to technology helping a company is keeping IT functions available and operational for use as much as possible. It is not possible to have 100% operational up time, so what is the best way to handle the times when they are not working? One very valuable solution is a help desk.

**What is a Help Desk and How is it Implemented?**

A help desk is a resource designed for IT users to contact when they are having problems with their IT services. Help desks institute a multi-tiered troubleshooting approach by having personnel with extensive technical knowledge available.

Implementation of this multi-tiered support varies widely within technology solution providers (TSP). In one TSP it may be one person with a wealth of knowledge carrying a cell phone. In another, it may be several people who perform some of the support in-house and several people from another company that are contracted for additional support.
What Standards Should Be Implemented By a Best Practice Help Desk?

The most strategic method of implementing a help desk is to follow Information Technology Infrastructure Library (ITIL) best practices. An ITIL best practice help desk must include:

- Single point of contact (SPOC) for IT interruptions
- Computer or software consultations
- Tracking capabilities of all incoming problems
- Problem escalation procedures
- Problem resolution

Implementation of best practices for help desk services is outlined in the service management best practices section of ITIL version 3. Specifically these areas include:

- **Knowledge Management**: A help desk should have a system that improves operational efficiencies by reducing the time spent to rediscover previous incidents or problems.
- **Problem Management**: A help desk should have a system that gathers information during incident management to help spot problems. This system will identify the root cause of frequent recurring incidents by capturing information in a knowledge base.
- **Access Management**: A help desk should act as the keepers of the user accounts along with password resets. Single ownership by the help desk will ensure quicker response time for end-users with user or password problems.
- **Service Catalog**: A help desk should have a published service catalog, ideally with pricing information included and with detailed service descriptions.

A Help Desk Will Assist in Enabling a Client to Meet Their Strategic Goals

Help desks are implemented in many different ways; however, by following the best practices outlined in ITIL v3, the help desk will meet the most important need of the end-user – it will get them operational as quickly as possible. In addition, by following best practices, the help desk will enable the enterprise to have a foundation for the IT department to not only meet the needs of the end-user, but for the IT department to link into strategic areas within the company. Thus, the help desk will be one component in enabling the enterprise to meet their strategic goals.

What Are the Critical Differences Between a Service Desk and a Help Desk?

The difference between a help desk and a service desk became more concrete with the writing of Information Technology Infrastructure Library (ITIL) v3, which was released in June 2007. Prior to version 3, the help desk and service desk were used interchangeably; thus, no significant differences between the two were recognized within the industry. ITIL v3 looks at the IT process from beginning to end and maps how it should be integrated into the overall business strategy. The service desk is a key component of the management of the overall process. The help desk is a component of the end-to-end process that is focused on end-user needs.
A Help Desk Focuses on End-User Needs

A help desk provides incident management to ensure customers’ problems are resolved in a timely fashion. A best practice help desk utilizes software to track the incidents making sure that no trouble gets lost. It manages a database that keeps track of the IT assets enabling access on a real-time basis to information about software and configuration of the IT system. The help desk has the ability to create monthly and annual reports on the number of troubles, the time to respond to the trouble, the time to fix the trouble, which could all feed into a service level agreement (SLA). Some of the specific tasks a help desk performs include:

- Computer or software consultations
- Change and configuration management
- Problem escalation procedures
- Problem resolution
- Single point of contact (SPOC) for IT interruptions
- Service level agreements
- Tracking capabilities of all incoming problems

A help desk is tactically focused and is most concerned about end-user functionality. One way of implementing a help desk is for the organization to meet minimum requirements to get an end-user back in service once an incident is reported. However, a best practice help desk utilizes processes and software to minimize the service interruptions both proactively and reactively.

A Service Desk Focuses on Client Strategy

A service desk is a single point of contact between users and IT service management. It manages information delivery by utilizing Information Technology Infrastructure Library (ITIL) v3 best practices to deliver these services both with software and defined processes. The service desk is the first contact in an organization for any and all IT questions. Best practices service desks are process-focused and company strategy focused. The processes outlined in ITIL v3 are broken down into five ITIL Core Service Lifecycles.

- **Service Strategy**: Evaluate current services and ensure a plan is in place to modify and implement new and existing services when required.
- **Service Design**: Evaluate and ensure a new service will meet current and future needs. Ensure a new service can be introduced into the live environment.
- **Service Transition**: Define a plan that ensures no service outages or gaps during a service transition, thus the effects of the transition on the corporation are minimal.
- **Service Operation**: Responsible for the ongoing monitoring of a service that is used to deliver services.
- **Continual Service Improvement**: Review and analyze opportunities to improve all IT processes and functions.

A Help Desk is a Component of a Service Desk
A help desk with ITIL v3 best practices is one component of the overall service management and will feed information to a service desk through software and process hooks. Specifically, the functions outlined in the service operations section of the ITIL core service lifecycles are help desk functions. These functions include:

- Event Management
- Incident Management
- Request Management
- Problem Management
- Access Management

These are not the only functions that a best practice help desk performs. There are additional help desk functions embedded in the other four segments of the lifecycle management (service strategy, service design, service transition and continual service improvement). For example, the help desk needs to be involved with any type of service transition to ensure the new service does not adversely affect the end-users.

Many Companies Have a Help Desk Without a Service Desk

There are some instances where a technology solution provider does not require or is not ready for the processes and service offerings of a service desk. In that instance, a help desk will meet the tactical needs of the TSP. The help desk will give users a place to contact when they are having specific IT issues. Thus, the amount of time an end-user is out of service will be minimized by the help desk.

Few Companies Have a Service Desk Without a Help Desk

The service desk is concerned with the overall IT process and the individual components that function and interact with each other on both a software and process level. One area that is a must in any IT service offering is the ability to manage specific end-user problems and issues. Thus, a service desk either has to have help desk functionality embedded in their service desk infrastructure or have the ability to link into a help desk offering for the end-user. The service desk is focused on corporate strategy and ensuring that all IT functions are currently working and will work in the future. It must also have the ability to ensure all end-users are up and functioning.

When Should You Use a Service Desk vs. a Help Desk or Do You Need Both?

Now for the tough question – should you use a service desk, a help desk or both? To answer this question, let’s review the highlights of each function. Before you proceed, also consider the desired effect on your business structure and goals. Service delivery applies to TSPs of all size and if carefully executed, can be the difference in prospering in the TSP business or just winging it day-to-day. Organizational size is not really a factor in service delivery since all areas need to be covered in some fashion to be successful. If you are a small provider, it makes better financial sense to staff a service desk person at a rate less
than a technical resource to handle the client facing aspect since not only is it more financially feasible, but a people person will be a better resource to communicate with clients over a technical resource.

**Help Desk is Technically Focused**

The help desk fixes problems that are taking place at that instant. Any time one of your employees is experiencing problems utilizing your information technology (IT) infrastructure, the help desk is contacted to fix the problem and get your employee(s) operational as quickly as possible. For this immediate response to end-user IT needs, the help desk must have employees technically trained in the appropriate technologies. The ultimate goal of the help desk is to offer first contact resolution as often and as quickly as possible.

**Service Desk is Customer and Process Focused**

A service desk offers a single point of contact (SPOC) and is focused on managing processes. The service desk is outward focused on the customer and inward focused on the day to day processes of the business. The ultimate goal of the service desk is to reduce client costs by having the appropriate personnel working on problems, by monitoring trends and by managing processes.

**Your Business Will Benefit the Most with Both a Service Desk and a Help Desk**

---

**SERVICE DESK SINGLE POINT OF CONTACT**

- Inbound Client Requests
- Dispatch
- Vendor Management
- Customer Follow Up
  - Validation
  - Surveys
Why should you use both? The help desk and service desk serve different purposes and both add value to your technology solution practice. It is obvious that a help desk is required; when something breaks you need to fix it. However, there are many instances when the help desk is getting a call and it is not of a technical nature. When this occurs, your company is paying premium dollars to a technical resource when one is not required—and that resource could be helping someone with a technical question.

This is where the service desk plays a key role in your business solution. The service desk will assist end-users with issues that are not of a technical nature. This allows technically skilled workers to stay available for the technical problems.

When done according to ITIL v3 standards, the service desk will be the single point of contact (SPOC) and route the call to the appropriate location for resolution. The service desk owns the call and will follow it through to ensure the customer who called in the problem is satisfied with the resolution. Having this SPOC and ownership of the call enables:

- **Higher end-user customer satisfaction**: The service desk is keeping the end-user well informed.
- **Increased end-user productivity**: The service desk is tracking the problem, enabling the end-user to continue with their daily work.
- **Better cost control**: The service desk ensures the call is being routed to the appropriate center within the company to be resolved.

The service desk also monitors all processes and trends. When the service desk notices problems within the processes or worrisome trends, they make adjustments to fix the problem before it is detected by the end-users.

To help differentiate between help desks and service desks, use the following questions to decide which describes your current operation most closely:

- Do you provide excellent technical support, helping customers to solve problems efficiently and effectively?
- Do you provide a single point of contact for all technical issues?
- Do you make changes to the IT infrastructure in an effective manner, but the method is informal and could be different according to the nature of the change?
- Do your support analysts wear many hats and diagnose problems, find the root cause and work successfully with others in IT to resolve the problem?
- Have you defined how you will offer technical support to your customers and communicated it to your customer base?
- Do you keep track of your IT assets and interface to your accounting system?

If you can answer yes to most of these questions, you probably operate a help desk!

- Do you provide excellent incident management, helping customers to return to productivity?
• Has your management embraced ITIL as the framework for IT processes?
• Does your support center participate in most IT processes and has that participation been formally defined?
• Do you have a formal change management process and a Change Advisory Board?
• Do you have a group distinct from the support center that performs problem management?
• Have you defined a service level agreement and published it to your customers?
• Do you keep track of your configuration items and the relationships among them in a change management database?

If you can answer yes to most of these questions, you probably operate a service desk!

There are three principal roles and associated responsibilities for the service desk according to industry best practices. However, some organizations might need to combine roles depending on the organization's size.
ROLES AND RESPONSIBILITIES WITHIN A SERVICE DESK

and structure and the underlying service level agreements existing between the IT department and the business it serves. It is important to remember that these are roles rather than job descriptions.

The following roles are required to perform the service desk processes:

- Service desk manager
- Service desk supervisor/senior service desk analyst
- Service desk analyst

**Service Desk Manager**

The service desk manager role is critical because it supervises tasks that are associated with the daily operation of the service desk, the continual development of the service desk function, and troubleshooting issues. These tasks are described below:

- Managing day-to-day activities
- Managing staff
• Producing staffing rosters
• Managing the service desk analysts
• Carrying out staff appraisals
• Producing and maintaining staff training plans
• Recruiting new staff
• Providing advice and guidance to customers and service desk analysts
• Producing management reports
• Representing the service desk by attending meetings as the service desk representative
• Maintaining the processes used within the service desk
• Developing new functions and processes
• Creating a service culture within the service desk
• Running awareness programs and campaigns to publicize the service desk and the services provided
• Developing processes and agreeing interfaces to other SMFs
• Liaising with incident and problem management processes regarding any changes in coding systems
• Planning the take-on of new services and workloads
• Providing input to SLA negotiations and reviews
• Working with other SMEs to ensure the availability and continuity of the service desk function
• Working with capacity management to ensure that sufficient capacity exists in order for the service desk function to meet service targets
• Defining and implementing new or improved working practices
• Troubleshooting issues
• Listening and responding to instances of dissatisfaction
• Liaising with customers and service level managers where service targets have not been met
• Discussing and liaising where incident or problem escalation is felt necessary
• Representing customer issues within the support organization

It is important that a person filling the troubleshooting position is always available during the working hours of the service desk. Therefore, it is typical for a service desk manager to delegate some of the day-to-day tasks. However, the service desk manager should retain overall responsibility of managing the operation of the service desk.

**Service Desk Supervisor/Senior Service Desk Analyst**

In small desks it is possible that the senior service desk analyst will also act as the supervisor; whereas in larger desks, it is likely that a dedicated service desk supervisor/senior service desk analyst role will be needed.
shift hours dictate, there may be two or more post holders who fulfill the role, usually on an overlapping basis. The supervisor/senior analyst role is likely to include:

- Ensuring that staffing and skill levels are maintained throughout operational hours by managing shift staffing schedules, etc.
- Undertaking HR activities as needed
- Acting as an escalation point where difficult or controversial calls are received
- Producing statistics and management reports
- Representing the service desk at meetings
- Arranging staff training and awareness sessions
- Liaising with senior management
- Liaising with change management
- Performing briefings to service desk staff on changes or deployments that may affect volumes at the service desk
- Assisting analysts in providing first line support when workloads are high or where additional experience is required

Service Desk Analyst or Technician

The service desk analyst or technician role is responsible for executing the day-to-day tasks of the service desk processes. This role is primarily involved with performing the incident management process. During the initial phases of the incident lifecycle, service desk analysts are responsible for ensuring that the incident is properly recorded, classified and given initial support. During initial support, they are responsible for resolving as many incidents as possible within the timescales allowed. Their actions at this stage have a very direct impact on customer satisfaction and determine how the incidents will be dealt with by the rest of the support chain.

Service desk analysts/technicians are responsible for assigning incidents that have not been resolved by initial support. However, their responsibility does not end at that point and they should retain ownership of the incidents, remaining responsible for ensuring that incidents continue to be progressed and escalated in accordance with service targets.

The analyst/technician provides progress updates to customers throughout the life of an incident. Once the incident is resolved, the analyst/technician will confirm that the initiator is happy with the resolution prior to closing the incident record.

The role also involves the initial processing of all types of service requests, proactive communication with the business and often the maintenance of self-service facilities, such as FAQ lists. This role is responsible for the following activities:

- Incident recording
- Routing requests to resolution groups when incidents are not resolved during initial support
• Initial support and classification
• Monitoring the status and progress toward resolution of all open incidents
• Keeping affected users informed about progress
• Escalating the process if necessary
• Resolution and recovery of incidents not assigned to resolution groups
• Resolution confirmation and closure of incidents
• Detecting potential trends and liaising with problem management where applicable

**Incident Manager**

• The incident manager is responsible for the effective implementation of the process “service desk and incident management” and carries out the respective reporting procedure
• He represents the first stage of escalation for incidents, should these not be resolvable within the agreed service levels

**Problem Manager**

• The problem manager undertakes research for the root-causes of incidents and thus, ensures the enduring elimination of interruptions
• If possible, he makes temporary solutions (i.e. workarounds) available to incident management and develops final solutions for known errors
• He engages in the avoidance of interruptions (i.e. proactive problem management) via a trend-analysis of important services or historical incidents

**Change Manager**

• The change manager authorizes and documents all changes in the IT Infrastructure and its components (i.e. configuration items) in order to maintain a minimum amount of interruptive effects upon the running operation
• The sequence of the individual stages is planned and communicated in order to recognize any overlapping as early as possible
• In the case of further-reaching changes, he involves the Change Advisory Board (CAB)

**Release Manager**

• As a central body, the release manager is responsible for the implementation of changes to the IT infrastructure so that they are carried out effectively, safely and verifiably
• Tasks include planning, monitoring and implementation of respective rollouts or roll-ins in coordination with change management

**Configuration Manager**

• The configuration manager prepares and makes available the necessary information about the IT infrastructure and services for service management
• To this end, he maintains a logical model containing the components of the IT infrastructure (CIs) and their associations

• Changes are documented and the updated state of the information is regularly checked

• As far as possible, he automates the update-process of the CMDB

ROLLES AND RESPONSIBILITIES WITHIN A HELP DESK

1st Level Support

• The responsibility of 1st level support is to register and classify received incidents and to undertake an immediate effort in order to restore a failed IT service as quickly as possible

• If no ad-hoc solution can be achieved, 1st level support will transfer the incident to expert technical support groups (2nd level support)

• 1st level support also processes service requests and keeps users informed about their incident status at agreed intervals

2nd Level Support

• 2nd level support takes over incidents which cannot be solved immediately with the means of 1st level support

• If necessary, it will request external support (e.g. from software or hardware manufacturers)

• The aim is to restore a failed IT service as quickly as possible

• If no solution can be found, 2nd level support passes on the incident to problem management

3rd Level Support

• 3rd level support is typically located at hardware or software manufacturers

• Its services are requested by 2nd level support if required for solving an incident

• The aim is to restore a failed IT service as quickly as possible
Support Considerations

While an internal service desk staff whose responsibilities are to support an internal corporate IT infrastructure may have little or no influence on establishing minimum requirements for the devices, operating systems, software applications and services they maintain in order to receive services, outsourced service providers are by far more fortunate.

Whenever possible, the technology solution provider should strive to establish and maintain minimum standards for service qualification. This helps standardize on hardware, operating systems, software applications and services, allowing the TSP to require their service desk staff to maintain proficiencies, skill sets and certifications on a controlled number of supported items, rather than a growing, ever-changing variety of systems and services. The benefits of this philosophy should be obvious, and include:

- More efficient and effective maintenance and incident resolution
- Easier end-user or client infrastructure setup and configuration of remote monitoring and management (RMM) tools and professional services automation (PSA) solutions
- Standardized performance metrics and reporting
- Faster on-boarding of new end-users or clients
• Speedier training and knowledge transfer by and between new and existing NOC and service desk staff

As a result of these and other benefits, end-user or client satisfaction is increased, and the technology solution provider and their service desk staff’s jobs are made much easier.

Some minimum standards required for a technology solution provider’s service desk to provide services for hardware, operating systems, software applications and services at end-user or client locations may include:

• Specific vendor-supported server, desktop and laptop hardware and BIOS versions
• Specific vendor-supported voice hardware and BIOS versions
• Specific vendor-supported operating systems and patch levels
• Specific vendor-supported cellular, smartphone and PDA hardware and operating system versions
• Specific vendor-supported routers, access points, switches and firewalls
• Hardware warranties for specific hardware
• Specific vendor-supported line of business software applications, versions and patch levels
• Specific vendor-supported antivirus, anti-spam and antispyware solutions, versions and patch levels
• Specific vendor-supported backup solutions, versions and patch levels
• Remote data storage
• Specific network security protocols and access controls
• Specific broadband requirements
• Other specific third party vendor relationships

In addition to qualifying the terms under which support will be provided by the technology solution provider to the client, it is equally important to establish the services that will be considered out of scope and specifically excluded from the service desk deliverables and SLAs. Some examples of out of scope services may include:

• The cost of any parts, equipment or shipping charges
• The cost of any software, licensing or software renewal or upgrade fees
• The cost of third party vendor, manufacturer support or incident fees required to deliver service
• The cost to bring the end-user’s or client’s environment up to minimum standards required for services
• Training services of any kind
• Maintenance of software applications unless specifically included in service agreement and SLA
• Servicing parts, equipment or software not covered by vendor/manufacturer warranty or support
• Failure due to acts of God, building modifications, power failures or other adverse environmental conditions or factors outside of the control of the technology solution provider
• Service and repair made necessary by the alteration or modification of equipment, operating systems,
software applications or services other than that authorized by the technology solution provider’s service desk staff, including alterations, software installations or modifications of any kind made by end-users, the client or their vendors, or anyone other than the technology solution provider’s service desk staff

• Programming (modification of software code) and program (software) unless specifically included in service agreement and SLA

It is important that any and all qualifiers for service such as these be clearly understood by the end-user or client prior to engagement and on-boarding by the technology solution provider or service desk. This will reduce misunderstandings and instead improve client satisfaction during service delivery.

DAILY ACTIVITIES

Many of the roles, processes, procedures, activities and responsibilities of an TSP’s help desk and service desk technicians are very much alike yet dissimilar, again, based on their respective areas of focus. The help desk daily activities are aimed at proactively managing and maintaining the efficient operating status of hardware devices, software operating systems and applications, as well as ensuring the continuity of services. The service desk duties are focused on managing the end-user incidents and problems. They both respond to incidents and problems that impact the users by following established service delivery protocols.

CHECKLIST

- Review service request
- Consult information documented in PSA solution as needed in order to perform incident management
- Qualify issue to determine if it can be resolved through tier 1 support within the
Based on best practices for proactive and reactive maintenance and service delivery, at a high level, the
general framework governing these processes is shared by both the help desk and service desk, with
differences surfacing based upon specific tasks. The following sections will reflect this similarity at a high level.

**Help Desk Daily Duties**

The help desk staff’s daily duties are determined by the technology solution provider’s help desk manager,
whose responsibility includes the management of the help desk and the proper identification, prioritization
and assignment of all alerts/service requests and proactive maintenance duties to the appropriate queue, tier
or resource.

In this context and since the TSP’s remote monitoring and management tool alerts generate service requests
in the professional services automation solution, the help desk staff’s typical day may resemble the following:

- Log in to the professional services automation solution
- Review all newly-assigned service requests to him/her
- Review any service requests previously assigned and still open to ensure they are not in danger of
  falling outside of SLA (the service dispatcher and/or help desk manager should be alerted to this status
  automatically by the PSA solution before it occurs)
- Work service requests in order of priority
  » Accept service request and time stamp
  » Review service request
  » Consult information documented in PSA solution as needed in order to perform incident
    management
  » Qualify issue to determine if it can be resolved through tier 1 support within the SLA
  » Work issue to successful resolution
  » Verify issue to be resolved
  » Document complete incident resolution details in PSA solution, mark status complete and
    time stamp
  » Service request is placed in 24 hour QA status for monitoring
  » Service request is closed once issue is determined to be resolved
- If service request cannot be resolved through tier 1 support or is in danger of falling outside of SLA:
  » Service request is escalated to tier 2 and successive tiers of support in accordance with the
    TSP’s service delivery process

All proactive maintenance activity is also scheduled, assigned and managed in the professional services
automation solution. Additional duties carried out by help desk staff may include:

- Review of monitoring reports to identify issues or trends that may impact service or business process
continuity for clients or end-users in order to address them in advance of potential interruption; or for capacity planning purposes

- Script or manually deliver required hardware, operating system, application software or service updates, patches and hotfixes
- Assist in new client on-boarding activities
- Customize, produce and deliver performance reports to internal NOC management
- Modify and tune alerting and thresholds on monitored devices, operating systems, application software and services in order to improve effectiveness and efficiency
- Manage, maintain and update internal, client and end-user infrastructure documentation, processes and procedures in the PSA solution

Service Desk Daily Duties

The service desk staff’s daily duties are determined by the technology solution provider’s service desk manager, whose responsibility includes the management of the service desk and the proper prioritization and assignment of all service requests to the appropriate tier. The scheduling of all service work is ultimately the responsibility of the service desk manager, but this and other functions may be performed by a service dispatcher. It is the service desk manager’s ultimate responsibility to make certain the service desk maintains their SLAs.

The service desk staff’s typical day may resemble the following tasks:

- Log in to the professional services automation solution
- Review all newly-assigned service requests to him/her
- Review any service requests previously assigned and still open to ensure they are not in danger of falling outside of SLA (the service dispatcher and/or service desk manager should be alerted to this status automatically by the PSA solution before it occurs)
- Work service requests in order of priority
  » Accept service request and time stamp
  » Review service request
  » Contact client or end-user as needed to gather any additional information necessary in order to begin incident management
  » Consult information documented in the PSA solution as needed in order to perform incident management
  » Qualify issue to determine if it can be resolved through tier 1 support within SLA
  » Work issue to successful resolution
  » Verify issue to be resolved to the end-user’s satisfaction
  » Document complete incident resolution details in the PSA solution, mark status complete and time stamp
Service request is placed in 24 hour QA status, after which the end-user is contacted to verify the issue has been resolved to their satisfaction and asked if the service request can be closed.

Service request is closed

- If service request cannot be resolved through tier 1 support or is in danger of falling outside of the SLA:
  - Service request is escalated to tier 2 and successive tiers of support in accordance with outsourced service provider's or internal service manager’s service delivery process.

As with help desk staff, service desk staff will also have additional duties to carry out, which may include:

- Review of service desk reports to identify end-user or equipment issues or trends that may impact customer satisfaction, service or business process continuity for clients or end-users in order to proactively address them.
- Assist in new client on-boarding activities.
- Customize, produce and deliver performance reports to internal service desk management.
- Manage, maintain and update internal, client and end-user infrastructure documentation, processes and procedures in PSA solution.

**SERVICE AGREEMENTS AND SLAS**

Developing a technology solution agreement is often the first step taken by a service provider in preparation for delivering services for a new client or prospect. Agreements are also routinely reviewed to ensure they are current and that all conditions are well spelled out. As with any legal document, agreements should be reviewed by a qualified law professional within your area of operation to ensure that all parties are protected equally.

Advantages to the service provider that are found in technology solution agreements include:

- Identifies what hardware, users, vendors and services are covered, as well as what is not.
- Clearly documents the client’s and provider’s roles and responsibilities.
- Accurately represents the client’s existing environment.
- Defines environmental prerequisites for service.
• Establishes a baseline for the environment
• Creates a framework to ensure the service provider’s profitability over time

The agreement also provides value to the customer as well, by way of the following:

• Provide the customer a comfort level required to engage for business
• Document the deliverables of the agreement
• Documents in clear and easy terms the provider’s services and how they are to be delivered
• Sets expectations to allow for success

**Service Agreement Considerations**

The technology solution provider’s service level agreement (SLA) is the agreement that binds their level of service between their service desk deliverables and their end-users or clients, and records the common understanding regarding:

• Services
• Priorities
• Responsibilities
• Performance
• Operation
• Response
• Guarantees
• Availability
• Serviceability
• Resolution

Agreements are commonly written to include SLAs in specific sections, along with service definitions, and may include:

• Definition of services
• Term of agreement
• Fees and payment schedule
• Taxes
• Coverage hours
• Exclusions
• Performance measurement
• Incident management process and response time
Services to Support SLAs

In this context, service level management is comprised of those processes, procedures and activities that manage and govern the delivery of service desk services to meet agreed-upon SLAs and are focused on the client, as opposed to service desk services whose focus is the individual end-user. In order to conduct effective service level management, the technology solution provider must conduct an effective business needs analysis in order to properly align deliverables with client needs, then continuously monitor and modify those deliverables to ensure they meet the established SLA with the client. The service level management process ensures that the service desk services are delivered according to the SLA. A properly configured professional services automation solution alone is not enough to support effective service level management – the technology solution provider’s service desk resources must properly deliver services and document all of their activity within it according to the provider’s established service delivery procedures. Only then can meaningful reporting be generated to evaluate performance against the SLA and demonstrate performance to the end client. In order for the technology solution provider to deliver uniform, measurable services in adherence to established SLAs and provide end-users or clients with a consistent, satisfactory support experience, they need to develop, implement and hold their staff accountable to effective qualification, on-boarding and ongoing service delivery and customer satisfaction processes and procedures.

VENDOR MANAGEMENT SERVICES

The Value of Vendor Management

Vendor management is the process whereby the technology solution provider manages all interactions with the end-user’s or client’s infrastructure vendors. This offloads that responsibility from the end-user or client and allows them to focus on running their business. This service adds tremendous value to the relationship between the end-user or client and the technology solution provider, as no matter whether through an
automatically-generated alert, or via the end-user or client generating a service request directly, any incident requiring third party vendor support for issues affecting their infrastructure is managed by the TSP.

All vendor management activity, including activity conducted by infrastructure vendors during incident resolution, is documented in the professional services automation solution by the service desk, per the outsourced service provider’s or internal service manager’s standard incident management processes and procedures.

This service saves the end-user or client the time and potential frustration of dealing with numerous vendors and also allows the technology solution provider to proactively manage all infrastructure vendor activity. The service desk works with these vendors directly to either quickly resolve issues or schedule on-site vendor visits, both of which have been found to tremendously improve efficiencies, incident response and resolution times, hence improving client satisfaction. End-user or client infrastructure vendors that the technology solution provider routinely agrees to manage may include:

- Line of business software vendors
- Telco/long distance/teleconferencing vendors
- Broadband vendors
- Fax/copier/printer vendors
- Web/application development/database vendors
- Structured cabling vendors
- Point of sale vendors
- Hosting/co-location vendors
- Equipment vendors
- Phone/VoIP system vendors
- Cellular/smartphone/PDA service vendors

In order to provide vendor management services effectively, the technology solution provider must provide all infrastructure vendors under management a Letter of Agency (LOA) signed by the end-user or client, which grants them the authority to act on their behalf, allowing them the ability to open service requests and schedule maintenance and repair services as necessary.

**REPORTING**

The Value of Reporting

The technology solution provider will integrate the remote monitoring and management tool’s reporting function with the professional services automation solution to generate rich, customized, consolidated reports for internal and external (or end-user or client-facing) purposes.
The technology solution provider will utilize specifically customized reports internally to analyze key metrics to evaluate service desk performance and modify internal processes and procedures to improve outcomes.

Externally, the TSP will utilize specifically customized reports with end-users or clients to validate the successful delivery of services within SLA and according to existing service agreements, as well as to identify opportunities to improve the availability or performance of existing devices, operating systems, software applications and services through activities outside the scope of the existing agreement or SLA. These activities may involve replacement or reconfiguration, which may or may not be conducted by the TSP, but instead by an outside vendor or other provider as deemed appropriate.

Report areas commonly available through a remote monitoring and management tool and professional services automation solution may include:

- Device, operating system, software application and service performance reporting
- Alert and service request reporting
- SLA performance reporting
- Call-specific accounting reporting
- End-user, client, service desk resource performance reporting
- Other customizable KPI reporting

When properly integrated and customized to provide meaningful data, these reports are a key tool utilized by the technology solution provider to improve the service desk's performance and efficiencies, yielding greater net profits, as well as increasing end-user or client satisfaction. When creating end-user or client-facing reports, it is a good idea to develop two versions – a very high-level executive summary and a more detailed report. In many cases, end-users or clients will prefer the executive summary report over the detailed report. Always have the detailed report available when conducting strategic meetings with the end-user or client, as you may wish to refer to it to dig deeper on specific topics during the conversation. When developing your executive summary report template, make certain to include as many visual elements to represent the data as possible. The more charts, graphs and visual elements and less text, the better since people tend to pay more attention to pictures over details.
CLIENT SATISFACTION

Due to the reality that service desk services are typically delivered remotely; and end-users, clients and the TSP’s staff may never have the opportunity to physically meet each other, it is critical for the provider’s staff to excel at interpersonal communications in all forms with clients, and especially verbal communications with them over the phone. Adhering to the established communication protocols will assist in reflecting a professional, courteous, efficient image for end-users and clients, fostering trust, loyalty and customer satisfaction over time.

What TO Say and NOT to Say

Being human like the rest of us, the technology solution provider’s staff will find themselves in situations when speaking with a client or end-user where they might say too much, or say the wrong thing, or say the right thing in the wrong way, or say the right thing, but in doing so contradict something that the client or end-user had been told previously by someone else. In any of these scenarios, a top-of-mind awareness and fear of accidentally doing any of these things during conversations with clients or end-users is required by all service desk staff.
Here are some things to keep in mind:

- Be courteous and professional and ask questions pertaining to the issue at hand – steer clear of idle chit-chat and volunteering too much personal information, such as what the service desk staff did over the weekend, last night, or inquiring the same of the client or end-user. This will help keep the relationship in the proper perspective.

- Refrain from volunteering potential causes of the issue or “thinking out loud.” When the issue turns out not to be caused by the service desk staff’s overheard suspicions, it may erode the perception of their competence by the client or end-user.

- Do not have internal discussions with other staff members on an open line – even though one service desk staff is handling their call professionally and following communication protocol, others may fail to do so in open conversation.

- Use the hold or mute button constantly – this is the safest way to ensure the client or end-user is prevented from hearing the wrong thing and allows the service desk staff to focus on resolving the incident as quickly as possible without distraction. Using mute allows the service desk staff to monitor the line, should the client or end-user wish to volunteer any useful information, or check status.

- Work behind the scenes or blank the end-user’s desktop during remote control sessions whenever possible. This practice helps reduce questions during the troubleshooting process and the potential perception by the client or end-user that the service desk staff isn’t competent because they are investigating so many different things during the troubleshooting session. While Automate doesn’t allow the blanking of screens, the behind the scenes command line tool allows this to easily be accomplished and your technicians will become more proficient at servicing the client when they are required to use this protocol.

- Don’t tell the client or end-user what you did. The more information is shared with the client or end-user, the more that information can be misinterpreted, misunderstood, or again, contradicts what they were told by someone else.

### Measuring Client Satisfaction

Customer satisfaction is notoriously difficult to measure for several reasons. To begin with, you have to count on customers to not only give feedback, but also to be honest in their assessment. Many people, when satisfied, feel no need to contact the company, while others will quietly grumble about flaws in service or products and swear off a company without ever seeking redress or voicing their complaints so that the situation can be remedied.

Requirements for satisfaction are not only unique to each individual customer, they can be extremely difficult to quantify, even on a personal level. However, if you are able to set standards for employee conduct where interactions with customers are concerned (both from a point-of-sale and a customer service perspective), then you can certainly implement procedures and guidelines to ensure customer satisfaction and measure their success. You can start by going to the source.

### Survey Customers

This is probably the only way to get customer feedback unless they contact you, which most people are too busy to bother with unless they are extremely upset about something.
You can provide surveys in several ways (through mail, email or over the phone) and in order to get the best information, you should allow customers to answer questions on a weighted scale (as in “rate your experience on a scale of 1 to 5, with 1 indicating complete dissatisfaction and 5 indicating complete satisfaction”). You may also want to survey repeat customers to see how their experience changes over time.

**Understand Expectations**

If you know what your customers expect from you, it logically follows that you will be better able to offer them an enjoyable experience. So make an effort to discover the expectations of your customers in terms of both service and products in order to ensure that you’re meeting their needs.

**Find Out Where You’re Failing**

If you’re not meeting customer requirements, you need to find out where the failure is occurring. Is your service less than what is advertised? Are employees making promises that cannot be met? Are customer service representatives dropping the ball on dispelling customer concerns and managing their complaints?

Whatever the case, it would behoove you to know where the lines of communication are breaking down so that relationships with customers can be mended.

**Pinpoint Specifics**

Whether a customer is satisfied or not, the data you collect will need to accurately assess what is working and what isn’t. So inquiries into level of satisfaction should include more than just the overall experience. You need to determine the products or services they purchased, what they liked or disliked about their sales interaction, how the actual purchase compared to their expectations and any suggestions they have for improvement.

**Assess the Competition**

If you don’t know why customers prefer another brand over yours, you cannot hope to keep them from flocking to the competition. So as part of your survey process, you may want to consider inviting customers to compare and contrast similar products or companies to find out what they are offering that you are not.

In contrast to regular user satisfaction, the best way to gauge a decision maker’s satisfaction is face-to-face during regular strategic meetings. It is important to set aside time specifically for measuring the client’s satisfaction, preferably at the beginning of these meetings. To assess the client’s feedback on your performance, you may ask questions such as:

- “On a scale of one to five, what is your overall satisfaction level with our services?”
- “Can you share with me why you rated us that way and what we can do to improve your overall satisfaction?” Or “Are there specific areas that we can improve on to raise your overall satisfaction level with our services?”
• “How would you rate your satisfaction level with our customer service?”
• “How would you rate the overall quality of our strategic business relationship?” “How would you rate your level of satisfaction with the value of our services?”
• “How likely would it be for you to recommend our services to another organization or business acquaintance?”

Although satisfying customers is an important goal, it is not an end in itself. It is a means to an end. The main goal is loyal (retained) customers because there is almost invariably a strong correlation between customer retention and profit. For most businesses, there is a strong correlation between satisfaction and retention although the linkage can be distorted by factors such as lack of product/service differentiation, extreme price competition and lack of customer interest and involvement in the product/service category. Satisfaction can therefore be seen as a necessary, but not always a sufficient pre-condition for customer loyalty. The diagram below illustrates how the interlock between satisfaction impacts this loyalty and eventually overall profitability in your TSP.

Retaining Clients

Many people may think offering discounts, free services or other monetary incentives will keep their customers happy. The truth is that it takes a whole lot more than simple discounts to keep customer loyalty high.

While there are various ways to build customer loyalty, below are three actionable components to help retain your customer base.

Set Expectations

Don’t wait to set expectations with current or potential customers – it will only hurt you. Clear expectations provide a framework for interaction moving forward and can really make or break a relationship. Knowing what to expect puts clients at ease and builds trust.

The main way that TSPs set expectations with their customers is through SLAs. It’s very important to put forward a clear vision of your services from the beginning, but it’s even more important to stick to your SLA. Managing client expectations is critical to the success of your business because that’s how your clients evaluate their experience with your company.

A great way to foster loyal customers is to “under promise and over deliver” on the expectations you originally laid out in the SLA. For instance, some TSPs state in their customer SLA that any ticket submitted with an “urgent” priority will be replied to within one hour. In reality, the response time on those tickets is closer to five to ten minutes. Delivery is critical; if you state it, you must deliver it.
Remember, the negative emotions customers feel from not having their expectations met will have a greater effect than the positive emotions from customers’ expectations being exceeded. Even if you deliver on your SLA nine times out of ten, I can guarantee that the customer will remember that one time you did not come through.

**Be the Expert**

The IT world changes constantly and it can be hard for the average business to keep up with emerging trends and new technologies. As your client’s “trusted advisor,” it is important that you establish a relationship where they feel completely comfortable seeking advice from you.

There is a lot of opportunity around this concept. Right now we are experiencing some major confusion in the SMB space around compliance/regulations and you have real opportunity to help your clients navigate the uncertainty. The unknowns become real opportunities to capitalize on. For example, if you can communicate the necessary steps to becoming HIPAA compliant, the client is going to recognize the value of your relationship, so if someone with a slightly better offer comes around, they are going to stick with you because they know you are an expert.

The TSP market is getting more crowded, which will result in increased competition across the board. So if specialization isn’t something you’ve considered before, it might be something you want to consider now; especially in fields that have a lot of regulation, such as healthcare and finance.

**Go the Extra Mile**

This seems like a no-brainer, but it is important to note. Now more than ever, SMBs are looking to have real relationships with their IT service providers. Going the extra mile fosters trust and builds long-term loyalty. It demonstrates commitment to your customers and you’ll end up benefiting from this in the long run. Your commitment will encourage clients to refer you to others. Customer referrals are one of the easiest and low-cost methods to getting new business.

Going the extra mile means paying attention to what your customers want. Think about what is important to your clients and what you can do to make their experience top-notch. A great experience will help you stand out from your competition and give you the edge when it’s time to renew contracts. Try to look for additional ways you can add value to your customers and they will love you for it and remain loyal to your company and brand for many years to come.
Today’s service desk technologies and reporting packages make it easy to capture copious amounts of performance data. Most service desk managers can tell you everything from last month’s average speed of answer to yesterday’s average handle time. But what does it all mean? If my abandonment rate goes up, but my cost per contact goes down, is that good or bad? Is my service desk performing better this month than it did last month?

Despite all the data that service desk managers have at their fingertips, most cannot answer a very basic question: How is my service desk performing? Perhaps worse, many service desk managers are unaware of the critical role – beyond mere measurement – that key performance indicators (KPIs) can and should play in the service desk. This includes the ability to track and trend performance, identify, diagnose and correct performance problems, and to establish performance goals and assign accountability for achieving the goals.
An increasing number of progressive service desks recognize that when it comes to performance metrics, less really is more. They have discovered the 80/20 rule as it applies to service desk performance measurement.

These world-class service desks have learned that the effective application of just seven KPIs is all that is required for measuring, managing and continuously improving their service desk performance.

**KPIs**

Many of us have heard the sage advice, “You can’t manage what you don’t measure.”

This is particularly true in the service desk, where effective performance measurement is not just a necessity, but a prerequisite for effective decision-making. Despite the widespread belief in this statement, few service desks use KPIs to their full potential. In fact, the vast majority of service desks use metrics to track and trend their performance – but nothing more! Unfortunately, in this mode, a service desk misses the real value of performance measurement by failing to exploit the diagnostic capabilities of KPIs.

The true potential of KPIs can only be unlocked when they are used holistically, not just to measure performance, but also to:

- Track and trend performance over time
- Benchmark performance vs. industry peers
- Identify strengths and weaknesses in the service desk
- Diagnose and understand the underlying drivers of performance gaps
- Prescribe actions to improve performance
- Establish performance goals for both individuals and the service desk overall

In short, performance measurement and management is a critical discipline that must be mastered for any service desk that aspires to world-class performance.

The average service desk tracks more than 20 metrics. A list of the most common metrics is shown on the following page.

This is a classic example of quantity over quality, where service desks falsely assume that they are doing something productive and good by tracking all of these metrics. The vast majority of these metrics, however, are only marginally relevant – at best! The seven metrics that really matter are as follows:

- Cost per contact
- Customer satisfaction
- Agent utilization
- First contact resolution rate
- First level resolution rate
- Agent satisfaction
- Aggregate service desk performance
These seven metrics represent the 80/20 rule when it comes to service desk performance: 80% of the value you receive from performance measurement and management in your service desk can be derived from these seven simple metrics!

One goal of every business is to achieve the highest possible quality at the lowest possible cost. It stands to reason, therefore, that cost and quality should be measured on an ongoing basis. In fact, many would argue that cost and quality are the only two things that really matter. In a service desk, the most effective cost metric is cost per contact and the best indicator of quality is customer satisfaction. With this premise in mind, it’s relatively easy to come up with the next two metrics on the list: first contact resolution (FCR) and agent utilization.

We have to ask ourselves, if customer satisfaction is one of the “foundation metrics” in the service desk, how can we affect it? How can we improve it? Put another way, if customer satisfaction is suffering, what is the diagnosis? Well, it turns out that customer satisfaction is affected by a whole range of other performance variables, including average speed of answer (ASA), call quality and handle time, to name just a few. But the single biggest driver of customer satisfaction by far is FCR! Nine times out of ten when customer satisfaction needs to improve, this can be achieved by increasing the FCR. This is why world-class service desks pay so much attention to this metric. They engage in a variety of tactics to continuously improve FCR, including agent training, investments in knowledge bases and agent incentives tied to improvements in FCR.

But what about the other foundation metric in the service desk, cost per call? It is common knowledge that labor (i.e. personnel) is the single biggest expense in the service desk. In fact, for the average service desk, 67% of all costs are labor related: salaries, benefits, incentive pay and contractors. By definition then, labor costs are the greatest lever we have to reduce the cost per call.

The best measure of labor efficiency is agent utilization. Because labor costs represent the overwhelming majority of service desk expenses, if agent utilization is high, the cost per call will inevitably be low. Conversely, when agent utilization is low, labor costs, and hence cost per call, will be high.

Most service desks commit two major mistakes when it comes to performance measurement: 1) they track too many metrics, and 2) they do not exploit the full potential of their performance metrics as a diagnostic tool.
PROCESSES WITHIN SERVICE DELIVERY

Incident Management

The service desk acts as the initial gateway into many of the IT processes, including the incident management process. The service desk acts as the interface between the business and IT and, in this case, between the business and the incident management process.

The service desk is responsible for the coordination of the incident management process. The service desk performs the recording, classification, and initial support phases of incident management. When incidents are assigned to resolution groups, the service desk retains responsibility for the ownership, monitoring and tracking of all incidents.

If the service desk is functioning successfully, many service requests and incidents may be handled and resolved without ever going outside of the service desk function.

Below is an example of automated incident management workflow that can be established by utilizing both an RMM and PSA solution coupled with your service or help desk.

Problem Management

The service desk, with its responsibility for coordinating the incident management process, is ideally placed to identify recurrent or multiple incidents that point toward an underlying problem. As such, the service desk is an important source of information for problem management.
In return, problem management works to identify and document workarounds and solutions that the service desk can use while performing initial support on new incidents.

When resolutions or workarounds are identified by problem management, the information is then passed to users by means of the service desk.

Problem management also aims to identify information that the service desk can use to proactively advise users. In the long run, effective problem management should reduce the number of incidents being reported to the service desk. The key process steps identified for problem management include identification and classification of problems, problem tracking and resolution, and problem closure.

**Identification and Classification of Problems**

Problems are typically identified through trend analysis of multiple incident reports and error logs. Alternatively, a high-severity incident also may be classified as a problem to enable detailed root cause analysis. Key aspects required at this stage include:

- Availability of all information that can assist in identifying the problem
- Different teams that must pool their knowledge and expertise to diagnose and resolve the problem
- Predetermined priority levels to ensure there is efficient allocation of resources

**Problem Tracking and Resolution**

A single tracking system — ideally interfaced with the incident management system — will assist in providing the audit trail and status required to monitor problems. In addition, communication to the impacted parties is critical at all stages to ensure there is an appropriate solution and timely resolution. Moreover, personnel must be trained to identify and track trends. In most instances, the root cause of the problem is identified only after a significant amount of analysis is undertaken. Tools such as Pareto charts and principles and Ishikawa diagrams (also called fishbone diagrams) are useful in identifying trends and the cause and effect of problems.

**Problem Closure**

Problem records should be closed when there is a successful resolution of the known error or if the business agrees to implement an alternate solution or workaround.

**Change Management**

Change management informs the service desk of any upcoming changes to ensure the service desk makes necessary preparations.

The service desk should be represented at CAB meetings in order to give their perspective to the assessment of changes and at post-implementation reviews to give their perspective on the success of changes.

As part of their role in proactive communications, the service desk can circulate the forward schedule of changes (FSC) and projected service availability (PSA) documents to customers.
The process for managing change is outlined below:

MANAGING CHANGE

Prepare Communication and Planning
Prepare

Design

Execute and Review
Transition and Change Management Plans
Execute

Sustain

Configuration Management

The service desk function uses the information from the configuration management database (CMDB) when performing many of its processes.

When calls are initially received, customer details may be acquired from within the CMDB. The service desk function checks these details with the customer to ensure that records are accurately maintained.

When processing incidents and service requests, the service desk function checks the configuration item (CI) details against those held within the CMDB and notifies configuration management where discrepancies are found so that they can correct the errors and investigate why the discrepancies arose.

The service desk function also utilizes the information within the CMDB to accurately target the supply of proactive communications to customers.

To be successful at configuration management, the TSP must incorporate these components into their routine which will ensure success.
**Configuration Identification:** This refers to the activities and processes dedicated to creating and maintaining full documentation describing configuration items (CI). A CI is defined as anything that has a function in the ICMS. The goal of configuration identification is to provide a unique identifier to each item to help track the changes to that item and to be able to understand its place in the system.

**Change Management:** This is the process, sometimes referred to as change control, by which the need for a change is identified, the impact of the change on the system (i.e. cost, schedule, operational performance) is analyzed, the proposed change is evaluated by a review body of corridor stakeholders and, if approved, the approved change is incorporated into the ICMS and/or existing network system with its appropriate documentation.

**Configuration Status Accounting:** This is the record keeping and reporting function of the configuration management process, ensuring that all of the relevant information about an item, particularly the documentation and change history, is up to date and as detailed as necessary.

**Configuration Audits:** This is a process of analyzing configuration items and their respective documentation to verify and ensure that the documentation reflects the current situation. In essence, while change control ensures that change is being carried out in adherence with the CM Plan, configuration audits ensure that the change was appropriately carried out.

**Risk Management**

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment.

Managing risks in a project is imperative for its success. We need to have a process (or processes) in place for risk management to be effective. Here are the five steps a TSP can use for risk management:
1. Identify Risks: Identify risks that affect the project (positively or negatively) and document their characteristics.

2. Assess & Analyze Risks: Assess the risk impact, analyze the probability of risk occurrence and prioritize the risks, numerically analyzing the effect of identified risks on project objectives (usually on cost, schedule and scope targets).

3. Plan Actions: Explore all the possible ways to reduce the impact of threats (or exploit opportunities). Plan actions to eliminate the risks (or enhance the opportunities). Action plans should be appropriate, cost effective and realistic.

4. Monitor & Implement the Action: Track the risks throughout the project. If risks occur then implement the risk strategy based on action plans. For example, if a mitigation strategy is selected, execute the contingency plan based on risk triggers. In case a contingency plan fails, execute a fallback plan.

5. Measure Effectiveness & Control the Risk Impact: Measure the effectiveness of the planned action and control the risk impact by understanding risk triggers and timely implementation of planned actions.

Risk management processes are cyclic, which starts from identification of a risk, and may result in identification of another new risk.
CLIENTS

Client Qualifications for Service

Not everyone out there is an ideal client for your business. It’s just the simple truth that there are some people who will not need your services or products, will not be able to afford you, will not be easy to work with and will otherwise not be a good client. The trick is being able to sort potential clients that you want to work with from the herd before you waste any time trying to deal with someone who simply isn’t going to be worth your time.
Before you can qualify clients, you need to have a clear idea of what sort of clients you prefer to work with. Without such an ideal, you don’t have anything to compare a potential client to. The characteristics of what you would consider a perfect client depend, of course, on your niche as well as the services or products you offer. However, there are a few questions that you can start with, no matter what type of business you operate.

- How much can your ideal client afford to spend? By having a clear idea of what you need to earn, you can automatically eliminate a lot of prospective clients who would not be a good fit for you.
- What sort of expectations will your ideal client have? You may find that a lot of otherwise ideal clients have either too low or too high of expectations and if you can focus your energies on those that will be truly happy with the service or product you offer, you’ll have a better chance of success.
- How long of a timeline is your prospective client working on? While your availability can change and therefore, the answer to this question that will qualify a potential client will also change, it can also eliminate a lot of problems. If you prefer to avoid rush projects, for instance, you can easily do so.

If you can write up a description of your minimum requirements for a client, as well as develop a good idea of what an ideal client looks like for your business, you’ll have an easier time of finding the clients you truly want to work with. Sticking to your guns on those minimum requirements can also help make sure that you’re taking on clients that will truly benefit you and your business. If you’ve been in business for a while, you probably have a few types of projects or clients you prefer to avoid, but that you’ll take on if you feel you have to. The simple truth, though, is that if you stick to those minimum expectations, you can move past clients who don’t meet them and focus your energy on landing the right clients. In almost all businesses, doing so will help you earn more.

Setting Minimum Client Qualifications for Service

Not all clients will qualify for the technology solution provider’s service desk services – nor should they.

In order for a TSP to deliver services effectively, efficiently and profitably, not only do minimum standards need to be established for the IT infrastructure to be managed, but for potential clients as well. Holding true to these client standards can mean the difference between building strong, growing, mutually beneficial business relationships with clients – or being contractually obligated to deliver services to difficult, noisy, slow-paying customers that do not value the time, dedication and effort required to support their infrastructure and users. Choosing to support the wrong client will cost an TSP more time and money than it is really worth – and burden them and their service desk staff with unnecessary bottlenecks and frustration.

Best in class providers may consider the following when determining a potential client’s suitability for services:

- Prior history and experience with other providers and vendors
- Overall company size/number of users
- Financial suitability, standing and creditworthiness
- Years in business or industry
- Staff attrition rate
- Client’s perception and value of the service relationship
• Existence of or willingness to create an IT budget
• Availability of and direct access to decision makers
• Willingness to provide necessary discovery information and access to key staff prior to formalizing a service agreement
• Willingness to invest to bring existing IT infrastructure up to minimum standards required for service
• Willingness to allow agent-based monitoring
• Willingness to share administrative credentials for systems and devices

The client’s history with other vendors, and specifically IT providers, will be a good initial indicator of their perception of the value of support services. If they feel the price to be paid to maintain their infrastructure and support their users is an annoyance and necessary evil to maintain their business, and they have an unusually active history of hiring and firing IT service providers, as well as a high staff turnover rate – these are obvious red flags to consider. On the other hand, if the client perceives the cost of supporting their environment and users as an investment that provides them a competitive advantage in their industry or target market, and have an existing IT budget (or are willing to create one), these are good signs.

The same thing holds true for potential clients that are very small in size. The client should be able to produce on average a minimum of about $2,000 in re-occurring revenue per month. Depending on your service model (per user or per device), this should average to about a minimum office size of 15 or so. If you consider the norm for support, each office will have the same basic three high touch users, whether they have 15 or 40 users, so you need to position yourself for success from the start to ensure you have enough revenue streams to afford the high touch users. If you accept a client that pays you $500 or $1,000 each month, you will still be burdened with the three high touch users and it will not be cost effective.

Technology solution providers also face having to squash service myths or negative client perceptions when dealing with difficult existing client or end-user situations. The best way to address this potential reality is to qualify prospects carefully to avoid engaging with difficult clients in the first place when possible.

Methods of reversing negative end-user or client perceptions may include:

• Reviewing and revising end-user or client-facing service delivery processes and procedures to improve interpersonal effectiveness
• Communicating more, and more effectively with end-users and clients
• Increasing anonymous customer satisfaction surveys and polling to identify areas for improvement – and improving them
• Sharing good news with clients and end-users, such as adherence to SLAs, positive testimonials or comments and improved customer service metrics
• Increasing face-to-face strategic meetings with the decision maker and discussing historical performance, positive improvements, and future goals and plans to achieve them
• Understanding the decision maker’s monthly, quarterly and year-over-year goals and reflecting service alignment, support and value in helping to realize those goals
In today’s society, where electronic communications fostered by email, Facebook, blogging, Tweeting and texting makes it easy to reduce verbal communications between individuals, the astute technology solution provider will redouble their staff’s efforts at increasing their verbal communications with end-users and clients.

Relationships are built and improved upon through verbal interpersonal interaction, not electronic communications. Because by their very nature service desk services are delivered remotely, and end-users, clients and the TSP’s staff may never have the opportunity to physically meet each other, it is vitally important to seek out ways to provide as much of a human touch as possible, whenever possible.

**SETTING MINIMUM INFRASTRUCTURE QUALIFICATIONS FOR SERVICE**

In order to maximize service delivery efficiencies, effectiveness, customer satisfaction and profitability, standardizing on and enforcing baseline environmental qualifications for the type and state of hardware, operating systems, applications software and services supported will serve the technology solution provider well. Although it may be more challenging for the TSP to enforce some of these requirements initially, over time it may be possible for them to establish and achieve a baseline standard within their clients’ organizations.

Standardizing on minimum environmental qualifications in order to qualify for service allows the technology solution provider to maintain their staff’s training requirements, certification levels and support specializations on a specific number of products and services. Instead of trying to support everything under the sun, which is impossible to do and a great way to miss SLAs and erode client confidence and satisfaction as a result, the enforcement of minimum standards for service, along with the establishment of supported products and services, improves service delivery effectiveness and customer satisfaction.
Hardware and Hardware Devices

In order to achieve standardization across hardware devices, the technology solution provider may consider the following and establish specific baseline requirements based upon the role of the hardware or device in the infrastructure:

- Type of hardware (server, router, firewall, switch, PC, laptop, smartphone, etc.)
- Brand of hardware
- A specific CPU type and speed
- A minimum amount of physical RAM
- A specific amount of free HDD space
- A specific BIOS type and level
- Hardware redundancy
- Warranty time period
- Specific physical connectivity types
- Specific local and remote connectivity methods
- Supported protocols and ports
- Physical security
- Access rights and security
- Specific configuration
- Specific WAN/LAN/DMZ location
- Interoperability with other local or remote devices

Operating Systems and Applications Software

In order to achieve standardization across operating system and application software, the technology solution provider may consider the following and establish specific baseline requirements based upon the role of the operating system or application software in the infrastructure:

- A specific operating system type, version and patch level (server, desktop, smartphone, etc.)
- A specific software application type, version and patch level (operating system, line of business, office productivity, etc.)
- Specific configuration
- Local and remote connectivity methods
- Supported protocols and ports
- Security methods
- Interoperability and ability to communicate with other local or remote systems, services, functions,
For a Microsoft Windows-centric environment, the TSP may establish the following baseline requirements for service:

- All servers with Microsoft Windows operating systems must be running Windows 2008 Server or later and have all of the latest Microsoft service packs and critical updates installed.
- All desktop PCs and notebooks/laptops with Microsoft Windows operating systems must be running Windows 7 or later and have all of the latest Microsoft service packs and critical updates installed.
- All server and desktop software must be genuine, licensed and vendor-supported.
- The environment must have a currently licensed, up-to-date and vendor-supported server-based antivirus solution protecting all servers, desktops, notebooks/laptops and email.
- The environment must have a currently licensed, vendor-supported server-based backup solution.
- The environment must have a currently licensed, vendor-supported hardware firewall between the internal network and the Internet.
- Any wireless data traffic in the environment must be secured with a minimum of 128-bit data encryption.

These minimum requirements serve as examples only. Ultimately – and based on a variety of factors, including internal capabilities, service deliverables and target market or client – it will be up to the technology solution provider to determine the minimum environmental standards they will require in order to qualify for their services.

**Connectivity Requirements**

In this context, connectivity requirements for service desk service delivery are defined as those services, devices and processes that allow the transfer of performance data and alerts from the remote monitoring and management solution at the end-user’s or client’s location to the technology solution provider’s service desk and/or datacenter, and provide remote access, control and desktop sharing capabilities to the technology solution provider and include network connections, equipment and services such as:

- Bridges
- Routers
- Switches
- Gateways
- Firewalls
- Broadband services
- Secure network protocols
Protocols

Protocols utilized by the technology solution provider’s service desk’s remote monitoring and management solutions to collect performance data and alerts for events, services and applications include:

- Windows Management Instrumentation (WMI)
- Network Basic Input/Output System (NetBIOS)
- Internet Control Message Protocol (ICMP)
- Lightweight Directory Access (LDAP)
- Kerberos
- Simple Network Management Protocol (SNMP)
- Syslog
- Extensible Markup Language (XML)

Security Requirements

Transmission of the aggregated performance data and alerts generated within disparate end-user or client networks from remote monitoring and management solutions to the technology solution provider’s service desk and/or datacenter is normally accomplished through secure protocols, and may include:

- Virtual Private Networks (VPNs)
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)
- Secure File Transfer Protocol (SFTP)

Services

In order to achieve standardization across infrastructure services, the technology solution provider may consider the following and establish specific baseline requirements based upon the role of these services in supporting the infrastructure:

- Type of service (Telco, broadband, hosting, Co-Lo, remote backup/storage, etc.)
- Provider
- Specific configuration
- Support/SLA
- Service availability and redundancy
- Service backup, restore and business continuity processes
- Communication and status reporting
- Security methods
- Interoperability and ability to communicate with other local or remote systems, services and functions
BEST PRACTICE UTILIZATION IN SERVICE DELIVERY

What Are Best Practices?

“Best practice” is a phrase used to identify a documented way of achieving a specific result under specific circumstances in an effective way. It is a concept based on lessons learned by one group that are then passed on to other groups. In this way, an individual or organization can focus on performance of the task rather than first determining the best way to accomplish the task. This can save both time and money. In addition, the use of best practices can facilitate a more consistent set of results for a technology solution provider.

The wheels of progress would turn much more slowly if every time an TSP began a task that they had never done before, they had to use a trial and error method to determine the most efficient way of performing the
task. However, by relying on other people's and/or organizations’ trials and errors that have evolved into a method that has been proven to be the most efficient, TSPs can begin the task using a proven method. The proven method, known as a “best practice,” can then be tweaked if necessary to meet the specific needs of their organization. This is the essence of best practices and why all providers should adopt this methodology within the confines of their organization. It is a proven or recognized technique that empowers the provider to be successful.

Four Key Elements of Best Practices

In most cases, best practices are scalable based on various facets of a given situation. Any number of variables could change the meaning of best practices for a scenario. Things like speed of network, number of nodes, number of users and physical layout of the network are just a few examples of factors influencing what goes into determining best practices in a given situation. Be aware of what factors were used in defining a scenario before using it for your own situation.

Best practices are a starting point; they are not necessarily meant to be hard and fast rules. If you have never done something before or are relatively new to a process, best practices provide a scenario to get you started.

A good starting point is not always the best stopping point. Because technology is forever evolving, so are best practices.

Why You Need Best Practices

Business best practices should be used to increase the value of each customer, regardless of the type of client they are currently. Utilizing best practices positions you to be the IT champion and helps move the client to the next level – and they will appreciate the results more.

To help illustrate why best practice methods are needed by technology solution providers, we will play a little game of Russian roulette – a game of chance in which a single bullet is placed in one chamber of a revolver, you then spin the cylinder and see if you get the lucky bullet. In this case instead of pointing the gun at your head we are going to introduce a new twist.

If I put one bullet in a revolver that contained six chambers and then spun the revolver, pointed it at your foot, and said I am going to pull the trigger now, how would you feel?

Now, if I told you I have a method that removes the bullet from the chamber, so the gun is not loaded, would you feel better?

The point of the story is many times we shoot ourselves in the foot in technology by doing something that is not the best practices way of doing it. Some people are just plain lucky; they always ignore best practices and never seem to shoot themselves in the foot. Other folks always seem to be shooting themselves in the foot and are left wondering what happened.
Take the bullets out of the gun and do it the best practices way. It may not always be the quickest, easiest or cheapest way to accomplish the mission at hand, but are you prepared to shoot yourself in the foot?

A best practice strategy can help your business avoid being shot in the foot by:

- Reducing costs and become more efficient
- Improving the skills of your workforce
- Using technology more effectively
- Reducing waste and improving quality
- Responding more quickly to innovations in your vertical sectors
- Becoming more competitive by establishing baselines
- Increasing sales and developing new markets by leveraging best practices in those areas

**How to Implement Best Practice Methods**

Think of implementing best practice initiatives within your organization as a project you would manage just like any other project. Research your options – there are lots of businesses within and external to your industry who are already using best practices – and definitely do not shortchange the planning process.

Follow these tips for a successful best practice implementation:

**Do Your Homework:** Research best practices of companies both inside and external to your industry to learn how they get things done – whether it is hiring employees, providing customer service or managing cash flow. Strategic partners such as Microsoft, VMWare, Cisco and Apple provide numerous resources centered on best practices.

**Communicate, Communicate and Communicate Some More:** Communicate with your employees about the best practice initiatives – who, what, where and why. Remember … you cannot over-communicate!

**Metrics:** What are you going to measure against? You need metrics in place to measure your progress. For example, if your goal is to decrease your average call resolution time from 11 minutes to eight minutes; that is the metric you’ll use.

**Change Management:** Have a change management component in place prior to implementation. Managing change means managing people’s fear. Change is natural and good, but people’s reactions to change are unpredictable and irrational. However, it can be managed if you are properly prepared.

**Modify For Your Business:** Modify the best practices of other organizations to specifically fit your business needs. Take the best of what you find and make the adjustments necessary so the best practice works for you.
Getting Everyone Involved: It is important to get your employees involved. After all, they are likely the ones most affected by the new best practice you are implementing. Lean on your experts to vet out your solutions and provide additional feedback on how they are being implemented.

It’s Your Business: If you get outside consultants and other experts involved, remember that it is your business – you bring the expertise about your business to the table; the consultants and other experts bring the expertise around best practice implementation. Be sure to align business objectives and customer needs as you nail down the exact practice to implement.

Keep Evaluating and Refining: Once you implement a new best practice, your work is not done. Evaluate and refine the best practice to keep meeting the changing needs of your business and your clients.

The diagram on the following page depicts several key areas of technology that should be reviewed for best practice methodologies. Implementing solutions around these areas will no doubt begin to set your technology solution practice apart from your competitors.
BEST PRACTICES FOR GROWING YOUR TECHNOLOGY SOLUTION PRACTICE AREA

What is the key to successfully growing your TSP practice and retaining customers so they will not go elsewhere for their IT needs? By keeping some key best practices in mind, you can differentiate your services so that you not only survive, but thrive in this challenging economic environment.
Here are five best practices for growing your technology solution business:

Understand Your Customers’ Business Culture: Get to know your customers’ way of doing business so you can deliver your services in a manner that best meets their needs. Don’t deliver cookie cutter services. Know how to tailor and execute your services in a way that is compatible with your customers’ unique way of doing business. This certainly doesn’t mean forgoing standards and processes, but rather allowing some flexibility when working to solve your clients’ issues and ensuring your service is exceptional in their eyes.

By having a keen focus on their customers’ needs, TSPs can offer higher premium services that add the most value to their customers’ business. This will enable TSPs to command higher fees and generate higher reoccurring profits, as well as entrench themselves in that customers’ business for years to come.

Education: Educate your customers on the value you are providing them and get them to move away from thinking about point solutions and day-to-day operational costs. If you can’t show value, you will always be competing on price and will struggle to build your niche in your respective market area. You are providing a valued-added service and you should be able to give your customers an ROI that will illustrate to them why you are the best choice for their business and that no one can compete against what you have to offer. If you can’t show them the metrics, you don’t deserve their business.

Customer Service: Commit to giving your customers better customer service than the next guy. Everyone provides customer service. Make yours exceptional. Your goal is to let your customers know that you are truly committed to doing whatever it takes to make them successful. Don’t make customer service an afterthought. Make it part of your overall business strategy. Go the extra mile and your customers will remember you for it.

Ongoing Communication: In order to retain their business over time, you need to maintain communication with your customers. Whether through phone calls, social media or on-site visits, you should strive to build a rapport with your customers so they see you as a trusted business advisor rather than merely a vendor. When other business opportunities arise, they will automatically think of you because of this trusted relationship you have earned and established.

Commitment: Commitment is the key to growing your business and adding value to your customers’ business. If developed properly, an TSP practice is a sophisticated business that needs to be given adequate dedication and resources. Whether you’re going into the TSP market in a big way or on a smaller scale, commit 100% to that level. Make the investment in the right people and the right technology in order to deliver the best value to your customers. Don’t do it halfway; you will only end up with unhappy customers and low profits.

TOOLS AND TECHNIQUES OF THE TRADE
Behind every great technology solution provider is a solid set of tools. Listed below are some essential tools for the TSP’s toolkit. You may have slightly different products you like, and that’s fine, as long as you’ve got the categories covered. These are tools that you need to invest in for your practice.

**Platform Tools**

These are tools that you use proactively across all your clients.

**Professional Services Automation (PSA) or Business Management Solution:** First, it is absolutely essential that
you have PSA software, which will provide you with the structure and functionality to actually run your TSP
practice. This includes everything from service tickets and agreements to invoices and scheduling.

**Remote Monitoring and Management (RMM) Solution:** This is your next critical tool. An RMM will monitor
your clients’ systems from a centralized console. It will enter tickets into your PSA, give you remote access to
your clients’ systems, allow patch management and provide scripting to automate simple, redundant tasks.

**Quote and Proposal Automation Solution:** A sales quoting tool will enable you to create professional and
accurate proposals quickly and easily, as well as tie into your PSA directly for end-to-end workflow and
processing.

**Antivirus/Anti-malware (AV/AM) Software:** It is recommended that you provide AV/AM as part of your
technology solution agreement, so you can control precisely what your clients are running. ESET is a great
solution, as it covers workstations, servers, Macs, and more, and its detection is very highly rated. In addition,
include Spybot or HitmanPro for malware detection and removal. You can also use Microsoft Essentials for
SOHO users who aren’t on your service plan, since it is free to companies with fewer than 25 workstations.

**Perimeter Security:** This is essential to a successful TSP practice and it is recommended that you include it as
part of your service agreement. Cisco ASA firewalls is a good option, but Sonicwall is very popular as well.

**Spam:** It is recommended that you choose a cloud-based spam service, which will also include email antivirus.
Reflexion and Roaring Penguin are two of the better options available.

**Web Content Filtering:** A cloud-based web content filtering solution is also recommended. Web content
filtering stops end-users from browsing to sites by category, such as known phishing and malware sites.

**Remote Access Tool:** A remote access tool should be included as part of your solution set. Round out your
solution set with a remote access solution, like ConnectWise Control.

**Reactive Tools**

The following tools can be carried by your technicians to troubleshoot issues that squeak by your platform.

**Malware Removal:** If your AV/AM solution is compromised, you need solid tools for clean-up. Consider
industry-leading security solutions, like BitDefender, Webroot, OpenDNS, and Malwarebytes.

**Network Troubleshooting:** If you’re having trouble with network performance or errors, consider network
troubleshooting tools. Try Wireshark for packet sniffing, Nessus for network discovery, Paessler PRTG for
network monitoring, and NSLookup for DNS Analysis.

**Drive Tools:** If you’re losing a workstation hard drive, there are a number of tools to use to try a recovery.
SpinRite can be used for drive maintenance, and Macrium Reflect or DrivelmageXML can be used for drive
imaging/cloning.

**ConnectWise Manage**
ConnectWise Manage allows you to organize your business around one system, enabling everyone in the business to connect and communicate through one unified and fully integrated operational platform.

Manage provides the features and benefits that VARs, TSPs, ISVs and web design firms not only look for, but require to get the most out of their business processes. You and your team can work with greater efficiencies than ever before. Manage simplifies roles and communication within your company including:

- Help desk and service management
- Sales, marketing and account management
- Finance, invoicing, and billing management
- Project management
- Procurement and inventory
- Dashboards and reporting
- Integration

**Service Board Usage**

A service board in ConnectWise Manage is the “bucket” that holds all of your service tickets. You can create as many service boards as you like, as well as specify the location and business unit that the service board is created for. By creating several buckets for your different categories of requests, you can organize and manage both external and internal needs. Some service board examples include: Alerts – Managed Service, Alerts – No Contract, Alerts – NOC, Help Desk, Internal, Requests – No SLA, and Sales. Don’t just think of it as a help desk function, but rather a source for managing all of your business processes.

**Statuses**

Statuses are used to define the various stages that can be assigned to service tickets on a service board. Statuses are used to determine if a service ticket will display on the board, whether or not time can be entered and if the ticket is open or closed. A workflow notification can also be assigned to each service ticket based on a status; this is known as creating a service status workflow. Examples of statuses that may be used include: New, New (Email), New (RMM), New (Tray), Reviewed, Responded, On-Hold, Waiting Vendor Support, Resolved, Closed and Canceled.

**Types**

Service types are used to establish types that can be assigned by the service board to service tickets upon their creation. The service type is also available to map revenue for general ledger accounts based on the service type the service ticket was in when it was invoiced. This means if you have a service type of “workstation” on the service board, you can map the revenue from all tickets in that service type to a certain income account in your general ledger.
Service types can also be used to track the amount of hours spent on a particular service. With this reporting, you may find that you spend more (or less) time on a particular service than you think.

If you are offering vendor management to your clients, consider setting up a service type for each vendor that you manage. This enables you to track the amount of time spent on a particular vendor. For example, if you are managing their copy machines, Internet service provider and voice over IP phone systems (VOIP), define these vendors as individual service types. Next, you can run the hours by service type report to analyze which service types (vendors) are profitable for you to continue to manage.

Consider creating a default service type labeled “Must Change.” This will help employees know it must be properly categorized by service type. These will also stand out on reports. Think about using service types as the general, high-level of technology that the service ticket is related to. Some examples of service types are: Mobile Device, Must Change, Network, Printer, Server and Workstation.

Sub Types

Service sub types give you the ability to further categorize the type of service requested. Some examples of service sub types are: Active Directory, Android, Apache, Blackberry, Citrix, CPU, File Server, Hard Drive, IIS, iPhone, Linux OS, MAC OS, Memory, MSSQL, NIC, Patching, RAID, Router, Switch, Terminal Server, VMWARE, Website, Windows OS and Windows Phone.

Items

Service items give you the ability to further categorize the type of service requested. It is also important to know that the standard service templates can be automated from this selection. Think about using this field to describe the exact action you are taking on the selected service type and subtype.


ConnectWise Manage and ITIL

ConnectWise Manage adds value to the ITIL v3 framework by supporting the processes that make up the five phases in the service lifecycle. In regards to ITIL, ConnectWise Manage can be the:

- Configuration Management System (CMS)
- Service Knowledge Management System (SKMS)
- Known Error Database (KEDB)
- Capacity Management Information System (CMIS)
- Supplier and Contract Database (SCD)

ConnectWise Sell

There are few critical processes in your business more important than your quote and proposal preparation software. The professionalism, branding and image, sales representation and pure impression created on
your clients that result from these processes echoes throughout your entire business and throughout your relationship with your customer.

**Sell** is the heart of creating the experience and business process flow for your customers and your sales team. With Sell, administrators and users have the ability to craft templates; manage workflow, integrations and documents; Order Porter templates; and much more. Many users opt for the rich capabilities of the Sell core for their daily work, creating and delivering the finest quote and proposal experience in the world.

With Sell you can:

- Reduce quote preparation time from hours to minutes
- Close more by delivering quick and great looking proposals
- Speed close rate when on-site by taking orders on the iPad®
- Easily add new productive sales consultants with repeatable process
- Have more sales that close faster

**Why We Need a Quote Tool**

We lost the deal? What happened? This sounds all too familiar. What’s worse is that business owners and sales professionals often don’t know that it is not about the money, but the proposal itself. A proposal is a solid reflection of the relationship you have with your prospect and having the right process will take proposal writing from an administrative nightmare to an efficient system of best practices where everyone wins.

A proposal is a document that solidifies your relationship with your customers. The proposal should identify the problems and document your solutions. In short, the proposal is a solutions document offering your company as the best solution, regardless of price. So how do you offer yourself as the best solution provider and what key things can you provide as evidence?

Ultimately, while “bad” proposals reflect poorly on you, “good” ones reflect positively on your business, your offerings and your relationship. A good proposal can help you stand out against your competition and promote you as the one solution provider who can solve your clients’ problems and help their business.

Below is a list of five steps that will drive success when you use a quoting tool:

- **Keep it Timely:** Using an automated quoting tool to replace your administratively slow process will allow you to be faster and more efficient. Timeliness is the first commitment in your relationship and sets the stage for the future tone of your relationship.
- **Create Standardized Processes:** Incorporating automated quote and proposal technology into your proposal process will streamline the typical chaos in your sales organization and your team will welcome the opportunity to easily and quickly generate a proposal instead of dread it.
• **Offer Meaningful Options:** If you expand the number of solution options to your prospects, you will find that they will tend to upsell themselves.

• **Image is Everything:** Just because the proposal is typed and you’ve used a word processing program with fancy bullets, does not mean it is professional quality. Your proposal reflects your company, its professionalism, its service and its dedication to doing everything to the best of its ability, and to the highest professional quality standards.

• **Integrate to Streamline:** Merge your proposals with your opportunity creation, sales management system and product fulfillment system. Integrate all of these systems into one smooth streamlined process and everyone’s work lives will be much better.

**Closure Time with Empowering Our Clients**

Order Porter combines the expertise and guidance of your sales team with your customer’s love of online commerce, option selection and configuration. ConnectWise Sell partners have revolutionized their sales process with Order Porter, compressing their selling timeframe, impressing their customers and achieving increasingly higher sales levels than ever before. Each time a client visits an Order Porter page, a notification is sent back to the quote preparer; thus, constantly keeping your sales team informed as to the level of interest in your proposal.

Completely template driven, Order Porter customizes customer-facing web pages, so you have the ability to utilize any type of content to represent your brand and image, marketing information, and other content to impress, educate, support and provide resources to your customer. Order Porter easily allows your customer to execute and document their order with an official and binding electronic signature with no additional effort on the part of your customer or your sales team.

**ConnectWise Automate**

*ConnectWise Automate* improves an IT solution provider’s service offering through remote support that results in improved technician efficiency, added flexibility and dramatic cost reduction while driving IT automation into your business.

With its latest features and enhancements, Automate delivers increased speed, real-time agent deployment status and unprecedented centralized visibility into customers’ systems.

In a nutshell, Automate can perform any IT support and management task or process that needs to be accomplished remotely, efficiently and non-intrusively. Cutting-edge, native agent technology makes Automate the most powerful, feature-rich and widely-sought RMM platform in the current IT market.

Automate delivers increased speed, real-time agent deployment status and unprecedented centralized visibility into customers’ systems.

If you can think of an IT task or process, Automate can do it. This Next-Gen technology is guaranteed to increase your operational efficiencies and dramatically improve technician performance with increased
visibility into critical data, enhanced manageability and a simpler setup process while growing your bottom-line.

What Does ConnectWise Automate Ignite® Provide

ConnectWise Automate Ignite brings you the highest level of automation out-of-the-box with pre-configured IT industry best practices, including groups, monitors, scripts, alerts, searches, templates and schedules based on Microsoft® best practices. ConnectWise Automate Ignite is an industry exclusive built directly into Automate that will drastically reduce and alleviate the learning curve associated with Automate, enabling instant time to value.

Developed by technology solution providers (TSPs) with more than 20 years of IT industry experience, more than 2,000 hours went into designing ConnectWise Automate Ignite to ensure it meets the needs of Automate partners by delivering:

- Navigation tree tailored to IT solution providers containing common searches, groups, templates and schedules
- Guided service ticket creation, file attachments and advanced time tracking for billing
- Full scale library of mission critical systems monitors based on Microsoft® best practices and focused on performance, availability and thresholds
- Automated scripting focused on auto-fix actions, scheduled system maintenance activities and IT best practice systems management
- Key system reports focused on Exchange environment, group policies and other back office system reports
- Automated patch management configurations based on industry best practices in a ‘set it and forget it’ mode and advanced cluster patching

Unlike other RMM solutions on the market, ConnectWise Automate with the industry exclusive ConnectWise Automate Ignite delivers features and functionality that no other RMM tool can provide and gives today’s IT solution providers the “must have items” to help maximize technician efficiency and their bottom-line.

Why Tickets for Everything

Anything that requires work from one of your employees or is an automated process from your RMM needs to be made into a ticket. The main reason is simple: tracking and empowerment. Consider this: if
your client calls in with a question about VPN, it could easily take 10 or more minutes of a technician’s time. Shouldn’t that time be tracked, especially if they’re not on a technology solution contract? When everything is tracked in a ticket, you are able to see how critical it is that you maintain organized and well-monitored service boards.

This assures that the correct people are looking at everything that requires work, and you can monitor important metrics like resolution and resolution times, and measure them against SLAs.

Aside from creating tickets for tracking or a permanent record of an instance, there are other valuable reasons for creating tickets. Think about the wasted time a technician encounters when looking for the root cause or related incidents that contribute to a particular item, such as an application crash. If as the TSP you are tracking software that is installed or uninstalled via tickets, a tech can easily and within seconds see that a customer has recently installed an office add-on and that is more than likely the root cause to why that customer is now having application crashes within Word. The tech simply reviewed the configuration and service ticket history within your PSA before he or she started the actual troubleshooting process, and found the ticket that shows the add-on was installed three days ago. Now instead of spending three hours reviewing and searching for the cause, the tech was empowered with information, enabling him to identify the issue very quickly and solve the problem efficiently.

Another very valuable piece to creating tickets for all tasks and automated processes is to build value with your client. Consider how easy it is for a customer in today’s financial times to lose sight of what value the handy TSP brings to their business. Imagine how simple it would seem if you paid $3,000 per month for service and needed to shave your budget by $2,500. By utilizing ticket creation and management, the TSP can easily demonstrate the true value that they provide to the customer and dispel any myth that the customer may have in regards to the service that is being provided. When the customer realizes that the $3,000 they are spending would equal, say, 30 hours of service and the last 90 days of history averages 45 hours of service per month (since you ticket
everything, including automation), how could they decide to try and cut back on expenses when IT services would actually increase if they attempted to reduce service levels?

Take a good hard look at your business, including all work that is done, all work that is requested and all processes. How many of those things are actually tickets? Now, take control of your service boards and ensure all of these items are tickets and that you’re tracking them. Trust us, you’ll see a huge improvement in efficiency and you’ll understand your clients’ businesses so much better.

**What Are Informational Alerts**

Informational alerts are another key area of ConnectWise Automate Ignite. Just as with monitors, these alerts generate tickets to keep a partner well informed, as well as build a history of repeatable reports and events. Several types of tickets fall into this informational category, including change control, configuration issues and reporting such as Exchange, SQL and best practice reports. When you consider the value that this sort of information can add to your service level, you can quickly see why it is being provided as part of ConnectWise Automate Ignite.

One advantage to reporting on change control issues other than to meet ITIL standards is to allow the partner to detect a potential detrimental configuration issue that perhaps the customer triggered by mistake. Without this level of change monitoring, the partner might not recognize a key service was removed or a vulnerable service was added until a much later time. This delay could result in a potential security breach or system outage for the partner’s customer and would more than likely generate that proverbial question from the customer – Why aren’t you monitoring my systems when I pay you to do that?

Aside from change control, it is also a good idea to report on configuration issues that surround your service delivery. This is built into Ignite so that you as the provider can be sure that the minimum setup requirements to deliver the service you are contracted to perform are setup within Automate. Prior to implementing this sort of informational alerting, partners routinely had issues with service delivery that were a direct result of missing items in the onboarding process within Automate. These alerts notify the partner on a regular basis that key settings have been missed and therefore, service delivery is impacted.

**Convergence Strategy**

The seamless melding of an astounding array of digital music files with a tiny, battery-free player – yes, the iPod is a marvel of modern technology. But that’s not why it’s hailed as one of the most innovative products ever, driving Apple’s impressive comeback in the personal computing arena. MP3 players with the same technology existed years before Apple introduced the first iPod. What gave the iPod its edge is the marriage of the iTunes online music service that allowed consumers to buy songs, rather than albums, with the user-friendly hardware. This is convergence in its simplest form.

Convergence is defined by Merriam-Webster as “the merging of distinct technologies, industries, or devices into a unified whole.” This is a powerful concept to a technology solution provider who is searching to maximize utilization and enhance operational efficiency within their organization. Can you imagine combining several components within your business to complete business processes and simplify tasks?
All technology solution providers should be constantly looking for ways to offer convergence within their business and to streamline the activities of their technicians. If you consider the amount of lost time your techs currently encounter by switching between various applications and screens on a daily basis, you will quickly see the need for convergence and the overall benefit it brings to your organization. One of the main goals I always had in reviewing a new application for my team was whether it integrated within the current footprint of applications we already had deployed. If a vendor provided an integration point that reduced clicks for my team, then that vendor was catapulted to the top of the review list because that solution was already on the way to making my techs more efficient.

The ConnectWise Suite

ConnectWise provides a seamless combination of solutions that gives you a 360-degree view of your business and clients, so you can increase efficiency and profitability with the power of automation. Designed as a hub and spoke model, ConnectWise Manage, the Suite’s business management solution, is at the center acting as a powerful database from which your client information is accessible to the other purpose-driven tools.

This dream team convergence of technology equips your business for success the way no other set of industry products can, because it eliminates the inevitable loss of data integrity that comes as a consequence of using multiple incompatible systems.

When you invest in the suite you can:

- Streamline sales, marketing, project management, and business processes with ConnectWise Manage
- Automate IT service delivery through remote monitoring and management (RMM) with ConnectWise Automate
- Maximize sales with quote and proposal automation using ConnectWise Sell
- Securely access and repair devices anytime from anywhere, with remote control through ConnectWise Control
- Manage, monitor, and bill Microsoft® Office365™ and Azure with ConnectWise® CloudConsole™
- Capture all communications in their respective tickets with ChatAssist™
- Discover and qualify sales leads with CampaignDirector™

With the ability to track and enter all billable time, and host it in a singular application (ConnectWise Manage), the suite also increases profitability. And when profit increases, businesses grow. The integrations within the suite are constantly evolving, and partners can expect to directly benefit through reduced clicks and automated processes to drive efficiency and a greater level of profits within their organizations.
What to Do After You Win That New Client

The Importance of an Effective Onboarding Process

Once the decision has been made to begin service delivery for a new client, the technology solution provider must execute an effective, efficient on-boarding process in order to meet client and end-user expectations and facilitate future service. A poorly designed and executed on-boarding process will quickly erode client and end-user confidence and satisfaction, and increase service delivery difficulty and cost for the TSP. No matter how you slice it, this is not the way to begin a new client relationship.

A successful on-boarding process begins before the decision is made to deliver services to the client. Read that again. Now think about this – it is not possible to on-board a client successfully if the provider does not collect the required data in order to set up the client’s account and configure the remote monitoring and management tool, professional services automation solution, billing and communications systems to support them.

Some of this data-gathering occurs during the initial business needs analysis meeting with the client, and more is collected during the technology assessment of their infrastructure during the pre-sales process. Of course, once the decision has been made to deliver services to the client, more information is gathered to complete the collection of data required to properly on-board the client.

The Business Needs Analysis

Early in the client relationship and during the pre-sales process, the TSP should conduct a business needs analysis with the prospect to gather the initial background information required to determine whether the prospect’s support needs can be met, and if continuing to explore the feasibility of building a business relationship with them makes sense. During this phase of the relationship, high-level information will be collected regarding the prospect’s infrastructure, including hardware, operating systems, application software, services and vendors. In addition, the prospect’s business processes and workflows will be discussed and understood, as well as their growth plans and business goals, along with their bottlenecks and pain points. This information, along with office and branch office locations and key staff roles and contact information will be gathered in preparation for the technology assessment that must be conducted, should the decision to move forward be made.
The Technology Assessment

The technology assessment is the next step in gathering more granular data regarding the prospect’s infrastructure in order to document and evaluate the hardware, operating systems, application software and services utilized in the environment, as well as their operating state and role in supporting the prospect’s business processes.

The TSP will leverage their chosen tools and technology, including the remote monitoring and management tool, to automate as much of the discovery and data-gathering process during the technology assessment phase as possible and evaluate the resultant output to qualify the infrastructure’s suitability for services.

Required Infrastructure Modifications, Updates and Upgrades

After the results of the technology assessment have been collated, the technology solution provider can compare the data against their established minimum requirements to determine what modifications, updates or upgrades will need to be performed in order to qualify the environment for services. After the required infrastructure modifications, updates and upgrades have been completed, client on-boarding can commence.

The Provisioning Process

In this scenario, the client provisioning process is typically characterized as those processes and procedures required to prepare the client, their end-users and their infrastructure to receive and participate in the TSP’s help desk and service desk services, and may include collecting all of the data required and conducting the following activities:

- Set up the client’s account in the TSP’s RMM tool, PSA solution, and communication and billing solutions, including all required supported user information
• If the RMM tool is agent-based, configure and deploy agents as required to monitor managed devices, operating systems, software applications and services per manufacturer or vendor recommendations and enable secure remote access and control and communications to and from the end-user or client location and the TSP's help desk or service desk

• If applicable, initialize a discovery routine by the RMM tool to identify all network-connected devices and their roles in the environment, or use other means to capture this information and document it in the RMM tool and PSA solution

• In the RMM tool, associate the applicable default monitoring templates to all managed devices, operating systems, software applications and services

• Develop base monitoring templates and assign them to all devices, operating systems, software applications and services that the RMM tool did not identify or does not have a default template for

• Configure, test and confirm the end-user's or client's ability to generate properly formatted service requests with all required information via email and the PSA solution's service desk portal

• Test and confirm proper two-way communications and alerting to and from managed devices, operating systems, software applications and services at the end-user or client location and the TSP's help desk or service desk

• Configure, test and confirm proper operation of the RMM tool's remote access and control function for managed devices and operating systems

• Configure, test and confirm proper two-way integration with the RMM tool, with raised alerts resulting in properly formatted service request generation, including end-user, device and client identification information, as well as correct status updating and alert cancellation occurring in the RMM tool upon service request resolution in the PSA solution

• Configure, test and confirm proper scripting and deployment of unattended operating system and supported software application patches and updates by the RMM tool

• Configure, test and confirm proper scripting and execution of unattended device and operating system optimization activities, such as deletion of temporary files and disk defragmentation by the RMM tool

• Customize and test client reports in the PSA solution

• Configure, test and confirm proper report generation and automated report delivery by the PSA solution; key infrastructure information required by the TSP for provisioning may include:
  » Client contact information
  » Server(s) information (type, make/model, role, warranty, support, OS, version, configuration, etc.)
  » Server application information (type, role, warranty, support, version, configuration, licensing, etc.)
  » Server services configuration information (IIS, DNS, DHCP, file & print, line of business, etc.)
  » Internal Active Directory information (AD Domain, administrator account, users and computers, etc.)
» Network shares, security and distribution groups, etc.
» Line of business application information (type, role, warranty, support, version, configuration, licensing, etc.)
» LAN and WAN information (devices, configuration, addressing, protocols, security, etc.)
» External Domain Registration information (provider, account, domain name, registrar, DNS, expiration, etc.)
» ISP information (provider, account, configuration, expiration, etc.)
» Web and email hosting information (provider, account, configuration, expiration, etc.)
» Router, switch and firewall information (type, make/model, configuration, addressing, support, warranty, etc.)
» Antivirus, anti-spam and antispyware information (type, vendor, role, warranty, support, version, configuration, licensing, etc.)
» Backup, disaster recovery and business continuity information (configuration, processes, etc.)
» Workstation, laptop and smartphone information (type, role, warranty, support, version, configuration, etc.)
» Application and productivity software information (type, role, warranty, support, version, configuration, etc.)
» Printer, POS and peripheral information (network scanners, faxes, document imaging solutions, credit card terminals, etc.)
» Other network-attached device information (type, product, service, role, account, warranty, support, etc.)
» Vendor information (type, product, service, role, account, warranty, support, etc.)

This information and more must be collected and archived in the TSP’s PSA solution in order to provide the help desk and service desk all of the information necessary to deliver services to the client in one managed location.
THE TRAINING PROCESS

Prior to service turn-up or go-live, the TSP’s help desk and service desk staff, as well as the new client and their end-users, need to be trained. Training should focus on key areas of service delivery for the service desk and help desk personnel and expectation setting for the client. If expectations are clearly set with all parties, the overall transition and service delivery will be very smooth.
Help Desk and Service Desk Client Support Training

Prior to service turn-up or go-live, the TSP’s help desk and service desk teams must become familiar with the new client’s infrastructure and its specific support requirements, along with any required modifications to established support processes for this particular client or their end-users, such as communication, escalation or status reporting processes.

Client and End-User Support Training

Prior to service turn-up or go-live, the TSP should typically conduct a training or multiple training sessions to indoctrinate the client and their end-users on their help desk and service desk’s processes and procedures for service delivery, as well as set the appropriate expectations in regards to response and incident management. Topics that may be covered during client and end-user training may include:

- How to open a service request (email, portal, phone, etc.)
- Service desk processes (incident, problem, configuration, change, risk, communication, release, service level, availability, capacity, service continuity, security, communication management, etc.)
- Service desk response and incident management-specific processes (issue identification, documentation, prioritization, assignment, remediation, escalation, completion, QA, closure, communication, etc.)
- Support tiers
- Service level agreement
- Customer service
- Reporting

Service Go-Live

After the TSP’s help desk and service desk have completed their client-specific training and the client and their end-users have received their support training, a service turn-up or go-live date can be established. This is the date that all systems, processes, services, help desk and service desk staff, and the client, their infrastructure and the end-users will be designated as ready to participate in help desk and service desk maintenance and support services.

The first thirty days after go-live with a new client will be the most critical for the TSP and their staff, as this is the time when the end-users will be the most critical and need to be won over by the new support relationship and its service delivery processes. If there are too many hiccups during this sensitive period, it may be difficult to recover the relationship. This is why it is imperative that the entire on-boarding process run smoothly, all processes be tested and validated, all required information collected and documented in the PSA solution and the help desk and service desk staff and the client and their end-users complete their individual on-boarding training prior to the decision to go live with the TSP’s support services.
30-45 Day Playbook

So many providers offer a 30 day free trial or a 30 day money back guarantee these days that one must wonder is this a requirement for our technology solution industry. Are these approaches necessary to win over business in today’s environment? Perhaps and perhaps not! In reality, if the TSP really focuses on the onboarding and customer experience during the first 30 days of the engagement, then offering a money back guarantee is a moot point because no one will ever ask for it. The key to success with winning clients over and retaining them is setting yourself up for success during this critical incubation period with the new client and ensuring they understand how the engagement is designed to work, as well as how everything fits together to define their service expectations.

Competitive crunch and convergence in today’s increasingly challenging service marketplace is fueling more customer churn and testing customer loyalty. TSPs face unprecedented challenges as cutthroat competition and new service models undercut pricing, prey on lucrative customers and disrupt established markets. Today, operational profitability is no longer enough. Business success is now dependent on delivering successful customer outcomes that increase loyalty and reduce turnover and the associated high costs of customer acquisition.

Customer satisfaction is the state of mind that customers have about a service, when their expectations have been met or exceeded over time. Hence, it is paramount to manage the customer expectations actively to achieve customer satisfaction. Achieving customer satisfaction in this first 30 to 45 days is a two-step process, which includes setting the client expectations and meeting or exceeding those expectations.

Communication is of critical importance during the early stages of the client process. This is when you will need to get to know the client’s business as well as possible. You’ll want to understand the products and services they offer, their corporate culture and what makes them unique to their customers. Additionally, you should get a solid understanding of their customers and what they will be looking for when delivering service to them.

Setting the client expectations is the first thing a technology solution provider must focus on following on-boarding of the new client. What transpires in this timeframe will be critical to your overall success as the client provider, as it sets the boundaries and helps your customer understand your delivery mechanisms. Key areas to include in this client playbook of services are as follows:

- **Communicate How Your Service Works and Train Your Clients’ Staff**
If you have a 24 hour SLA, is that 24 clock hours or three business days? If this is not documented and explained to your clients, you are leaving it to their interpretation. If you have to pull out your contract, you have lost points with the customer even though they signed it.

Do you use Automate Tray to communicate new issues back to your service desk? If yes, you need to explain to the client how this works, as well as if this method of communication receives any priority when it comes to service. Some TSPs utilize this method of communication in return for priority service since it proves to be a more efficient method of communication than telephone calls or emails to your service desk. In this case, the TSP sets up a special service board within their PSA and routes all incoming tray tickets to that board so they can prioritize those tickets and provide a better level of service to those customers utilizing that method of ticket creation.

Another key area that must be communicated to new clients surrounds maintenance windows. Maintenance windows are designed to provide clients with a timeframe of when maintenance tasks will be performed to allow them to prepare for possible disruptions in advance. Typically, maintenance windows will be planned for a time where activity is at its lowest so as to cause minimal disruption. Customers need to be made aware of the planned schedule, as well as understand the potential impact to their business from rebooting machines during these windows. The last thing an TSP needs is to be explaining why they caused a level of data loss by rebooting something that had an application open at the reboot time. If you do a good job of explaining to the client that machines need to be available and online during this timeframe, as well as that machines should be restarted at the end of a shift, it will reduce the risk of disruption when maintenance and reboots are needed.

**Address Immediate Concerns**

If the reason you were hired is that the printer in the corner is consistently offline, it is important that you address the issue in the first 30 days with a plan of attack. If the plan does not work, they will at least know you attempted to address the issue at hand; big picture replace the printer if you have to, but fix the issue that got the last provider fired.

Is there anything more exasperating than telling someone what you want or what your problem is and then discovering that the person hasn’t been paying attention and needs to have it explained again? From a customer’s point of view, I doubt it. Let go of the sales pitches and the product babble. Let your customer talk and show him you are listening by making the appropriate responses, such as suggesting how to solve the problem. Dealing with concerns that have been voiced will set you up to succeed in almost every instance.

**Set Expectations**
Have you ever worked with a customer who held unreasonably high expectations for you and your business? High expectations, that were never addressed or part of the contract? It’s a common problem that has a very simple solution. Before the sale, set clear customer expectations to establish a strong and sustainable relationship with your client. When setting expectations, timing is everything. If you wait until after the sale is made, the client may feel as though you weren’t being honest from the beginning.

Communication is key to a lasting relationship with your clients. And to exercise good communication, you must set expectations not only early on, but also during future projects to maximize opportunities for success. There’s a popular saying that goes, “If we can’t define it, we can’t measure it, and if we can’t measure it, we can’t manage it.” By setting expectations, you 1) minimize the chances of error via miscommunication, 2) assign responsibility and accountability, and most importantly, 3) define an accurate project scope for both you and your client. So take some time and look over these important steps that will help you establish expectations with your clients.

Establishing Roles: Discuss Your Capabilities, as Well as Your Limitations

First impressions are always important and they certainly apply when setting expectations about what you can do for a client. When a client calls or emails you, it’s important to be straightforward about what services you do and do not provide. If you can provide excellent front-end development, but you don’t have a familiarity in e-commerce, don’t be afraid to state that. Your clients shouldn’t expect you to be savvy at everything and you shouldn’t pretend that you are either. It occurs frequently, where a party acts upon the assumption that the other party member can or cannot do something. As a result, scopes unexpectedly change and trust is broken. This rule of setting capabilities and limitations applies both ways. Don’t assume that your client will provide all the necessary content and assets on X day. Be realistic and discuss what’s possible and what’s not — and identify potential weak points that can be resolved through early and smart planning. Otherwise, you’ll be left with the consequences of delayed response times, disappointing deliverables and missed expectations.

Establishing Duties and Participation: Identify the Point of Contact and the Frequency That You Will Be Communicating

It may seem like an unnecessary question to ask someone in this age of technology and high-speed connection, but you’d be surprised how difficult it can be to reach the right person at a time when you need them the most. It’s important to identify the main point of contact you should go to for general communications, questions and concerns for your project. If there are other special needs and circumstances for communicating, such as talking to the CFO or another senior management member, be sure to get introductions done early in the project as well. If you’re one of four members on a team, make sure you designate the point of contact on your side as well so that all channels of communications remain efficient and filtered (to prevent superfluous and unnecessary disruption to others).
In addition to determining the point of contact, it’s critical that you determine frequency of contact and expected response time with your client. If your workflow involves a very iterative process that requires a lot of prototyping and progress checks, make it known that you will be contacting your client frequently and that you will be expecting a more participatory role from them early on in the project. If you’re prone to sending preliminary designs first thing in the morning, inquire if you can expect a feedback response by the afternoon so you can plan your schedule accordingly on when would be the most efficient time for you to do revisions.

**Iteration and Confirmation: Repeat Your Understanding of Things to Prevent Misinterpretation and Miscommunication**

It’s pretty easy to hear and interpret what someone has to say, only to later discover that what you thought you heard wasn’t what they meant at all. Whether it’s due to ambiguous communication on their part or a misunderstanding of your own, misinterpretation can easily happen if you’re not careful. Prevent these mistakes from becoming problems by reiterating, in your own words, the key points of the conversation. This is a great practice, not only in person, but on the phone and over Skype as well. It is also recommended that all verbal communications be followed up with a written synopsis to ensure clarity and accountability.

Also be sure to practice iteration and confirmation when your client is trying to explain something to you, like a description of a particular visual aesthetic they had in mind or when they’re simply expressing their opinion on something. You’ll quickly learn that not everything you hear is what you think it is.

Remember that you’re the expert. Therefore, you should always be proactive in setting expectations on whatever the next courses of action should be — whether they depend on your clients’ actions or your own. Setting next steps reassures your client that 1) you’ve got a good handle on where the project is at, 2) their wishes and expectations are being met, and 3) everything is still progressing at an optimal pace. On an additional note, communicating the next steps ensures you retain responsibility for keeping the project on course and hold your clients accountable for any dependencies they are responsible for.

**Exceed Established Client Expectations**

When it comes to pleasing clients, there is no substitute for high-quality work and a cooperative attitude. After all, that’s what you’re being paid for. But everyone knows that’s not the whole story. As a technology solution provider, you have to distinguish yourself from other contractors in ways that go beyond the essentials, especially in a down economy.
Here are a few secrets to surpassing clients’ expectations that will keep you ahead of the competition.

Agree to a Deadline You Know You Can Beat: Clients nearly always appreciate when good work arrives before the due date, because it affords them flexibility. Plus, it shows that you are both efficient and customer-focused. Of course, you shouldn’t nudge clients to begrudgingly accept deadlines that do not suit their needs just so you can exceed expectations later. But the surprise of early delivery is more memorable than an up-front offer to beat a client’s proposed due date.

Be an Astute Questioner, Not a Silent Sage: People often overestimate the value clients place on not being bothered while their work is with a contractor. In fact, asking pointed, proactive questions during the process demonstrates your genuine interest and focus. That doesn’t mean nickel-and-diming clients so they suspect you have obsessive-compulsive disorder, but follow-up that proves you have foresight and a knack for process efficiency sends the reassuring message that while the work is in your hands, there’s no need to worry about it. Silence, in contrast, can generate unease. Besides, the occasional question is a pinprick compared with the laceration that a wholesale misinterpretation can later prove to be.

Be Collegial: You’re probably thinking, “Duh, I’m obviously not going to be rude.” But collegiality is less about politeness and more about your level of deference. Too much deference, which is what most TSPs show, makes you seem merely like the hired help rather than a capable complement to the internal staff — and that doesn’t inspire confidence. Most clients would rather work with an equal (i.e. a colleague) than a lackey, especially if you’re providing expertise. That being said, acting like a know-it-all obviously isn’t collegial either.

Offer Constructive Suggestions at the End: Every process can be improved and who better to provide insights than someone who just went through it? If you focus solely on the merits and not on how you would benefit, your ideas for improvement won’t sound presumptuous or like complaints. A truly useful suggestion offered in good faith and with great tact is one that the client will want to implement, probably with you. Of course, making suggestions as an outsider is a delicate endeavor that requires appropriate circumstances and good social skills. But if you’ve got both on your side, the payoff can be big.

Finally, document the additional things you have done in the client’s environment that were not on their radar or things they didn’t even notice were an issue. You should also document items that you are addressing as issues as they occur and are remediated with auto-fixes to show that you are being proactive by pushing out your standardization into their environment. The history of services that you create will go a long way towards showing that you are constantly exceeding the expectations of your client.
Report Improvements

The last critical step in this initial 30 to 45 day client incubation period is reporting back to the client with the improvements that have been made. The key areas to focus on when it comes to reporting back to the client are as follows:

- **IT Investment Planning**: Help customers make better business decisions and plan for future IT investments.
- **Differentiate Your Offering**: Tell your story clearly and concisely to strengthen your value proposition.
- **Maintain and Increase Service Levels**: Use reports to understand how mission-critical business services are performing.
- **Leverage Reports as a Sales Tool**: Drive higher-value business by showing customers how you can reduce their downtime costs.
- **Become a Trusted Advisor**: Earn your customers’ confidence by effectively managing their IT and measuring results against SLAs.

When reporting, it is also essential to ensure that the data being reported is consistent. In other words, don’t report one set of data in a pre-sales campaign and then at the 30 or 45 day mark present a different report to the client. This only serves to confuse the picture. Thus, all reports being utilized for customer reporting should be presented in a clear and concise manner to ensure the client doesn’t become confused by what data is being reported on.
LEVERAGE AUTOMATION TO PERFORM CONSISTENT, REPEATABLE SERVICE DELIVERY

Automation and Your Service Delivery

Automation is what drives efficiency and profitability within technology solution practices. RMM tools, like most IT systems, are inherently automation engines in themselves that contain the capability to reproduce processes and answer cause and effect situations. Some tools do an exceptional job of leveraging this capability while others fall short even though they attempt to capture the essence of repeatable tasks. In all cases, the automation can be tailored specifically to the exact environment of the organization. On the down-side, it can be time-consuming to find the necessary skills either internally or in the marketplace to accomplish this.

Mastering the automation will allow your business to not only be able to offer repeatable service, but do so in a very controlled and organized fashion. This improves customer satisfaction levels and allows business owners to sleep at night knowing they are doing an effective job of maintaining client systems. The correct incentive for applying automation is to increase productivity and/or quality beyond that possible with current human labor levels, so
as to realize economies of scale and/or predictable quality levels. The incorrect application of automation which occurs most frequently is an effort to eliminate or replace human labor. Simply put, whereas the correct application of automation can net as much as three to four times the original output with no increase in current human labor costs, incorrect application of automation can only save a fraction of current labor costs.

The often untapped power of ConnectWise Automate is the ability to build an automated response system to manage your clients’ IT systems. Tapping into the power of automation is the largest hurdle that a technology solution provider must overcome to make service delivery a success. ConnectWise Automate is built from the ground up with automation in mind and includes the key components to facilitate the delivery of automated services. The components within ConnectWise Automate that empower you are reflected in the diagram on the following page.

**How ConnectWise Automate Empowers Your Business**

As you can see in the diagram, ConnectWise Automate offers many pieces that fit together to provide a solid foundation for creating automation within your organization. All of these pieces can be leveraged to build a complete automation approach and provide a consistent platform for service delivery.
Manage the Forest Instead of the Trees

To make automation a success, the best approach is to manage systems by way of a policy based management plan versus an agent or client management plan. To accomplish this, all of the components above are linked together by way of groups acting as the foundation for the automation and each of the others lends to the overall process and repeatability of the system.

Groups

Groups are an easy way to organize and maintain the needs of your clients and are the foundation for creating an automation solution to service your clients. Scripts, monitors, patches and other management tools can be implemented at the group level for specialized service agreements. Groups apply settings to the remote agents based on their respective agent templates

- Groups are used for configuration, sorting, permissions and managing services. Create as many levels of groups as you would like.
- To add computers to the group, use auto-joins based on searches.
- Scripts and software deployments can be scheduled on the group and will be executed on all the members of the group.
- Monitors can also be setup on a group and installed or removed from every computer in the group.
- Patches can be approved at a group level.
- Templates can be set on the group and will apply to all of the computers in the group.

Automating group membership is the key to setting up a repeatable and consistent automated approach. To accomplish this, you must include two key items as groups are built out: Auto Join Search and Limit to Search. These items are the foundation to keep the systems within the group consistent and true.

Master, Non Master and Greyed Master Groups – How Do I Choose?

- **Master**: Remove the agent from all other groups when the agent is joined to a master agent
- **Non Master**: Member agents can be removed from the group when the agent joins a master group
- **Greyed Master**: Greyed master group agents will not be removed from the group when the agent joins a master group

Groups act as the hub in the automation setup of ConnectWise Automate and certain groups should be used to deploy various types of monitoring and maintenance to achieve an overall best practice approach to monitoring. The basic rules as defined by ConnectWise Automate Ignite are as follows:

Service Plan Groups

- Routine scripts that apply to all members on a regular basis
- Generic software installation scripts
- Internal monitors that are group specific
- General remote monitors that are group specific
Server Role Groups

- Specific scripts that apply to all members on a regular basis
- Specific role based software installation scripts
- Role based remote monitors that are group specific

Patch Approval Groups

- Patch scheduled installation time
- Patch scheduled reboot time

Extra Data Fields

Extra data fields serve multiple purposes within the ConnectWise Automate architecture. They can be used internally for extra data recording or can be indexed and used externally. These extra data fields can be used in creating scripts and searches. For example, you can create an extra data field to exclude specific patches from being installed and tie this into your patch process. With this checked, these patches can be part of an auto-join group to automatically place them in a selected group which will allow the segregation of these from the patching process. Additionally, custom commands can populate these extra data fields with return data.

Extra data fields can be added to the following screens:

- **Computers**: Computer > Info tab
- **Locations**: Location > Info tab
- **Clients**: Client > Info tab
- **Probes**: Computer > Network Probe tab
- **Network Device**: Network > specific device > Main tab
- **Tickets**: Tickets > specific ticket > Ticket Data tab
- **Groups**: Groups > specific group > Info tab

Extra Data Fields as Found Under Dashboard > Config > Configuration > Additional Fields
Extra Data Fields Cautions

- Extra data fields may take up to six minutes to show up in the search creation screen or for data to appear in search results
  - In ConnectWise Automate, triggers will fire upon field creation or saving data within an extra field that refresh the extra data field views
  - To force an update of these tables, select Help > Server Status > Load Properties and Views
- Never change the data screen field of an EDF that has data stored for it
  - For example, never change an EDF from Client to Location screens; always create a new field in that case

Searches

Searches allow you to build queries without worrying about knowing MySQL or the ConnectWise Automate database structure and can be used to run impromptu reports or find similar computers for upgrades. The searches that you define can be saved for later use and can be used for group auto-join scripts, group scheduled apps and scripts. Once a search is created, it cannot be edited; only deleted and recreated.

- All database relations are preset by the search editor
- MySQL wildcard operators % can be used
- If you are modifying a search, save the search as a new search so future updates to the original search do not override your modifications
Complex Search Query

Because searches are easy to utilize, we need to examine why using the Auto Join Search capability at the group level is so important in maintaining a consistent delivery. These factors all apply in this case:

- Drag and drop is full of potential errors and auto-joins remove this capability automatically
- Auto-join searches give a consistent, predictable result
- Auto-joins let you drive a consistent policy to your agents
- Auto-joins rebuild every 30 minutes – select run now on the group default tab to run immediately
- Limit to Search removes agents that are not returned in the search results

Templates

Agent templates pertain to agent configurations and are used to apply certain rules to sets of computers. ConnectWise Automate comes packaged with several default templates that are automatically applied to the corresponding group.

- Templates are applied to an agent to build an effective policy that is pushed to the agent at its configuration
- Template priorities are 0-10, where 0 is the highest and 10 is the lowest priority to apply the template settings
  » Templates should be applied in logical layers allowing you to build granular settings to apply to your agents
  » Use Group Template Priorities to weigh your more important templates when applying them to groups
Template Cautions When Using Drag and Drop

Group auto-joins reapply the latest templates (Effective Policy) on each auto-join.

- Drag and drop only applies templates on the group when the agent joins or if you force an apply of the template
- Auto-join enables template changes to be automatically updated
- If you have a drag and drop group, by default the existing members of the group will not receive a template update, but new members to the group will receive the update

Scripts

Scripts can not only make your work go faster; they can make your job easier. Scripts are one of the most powerful features in ConnectWise Automate. They can be used to perform ordered functions and combine with other features. Some common uses of scripts are:

- Automate software deployment
- Modify computer settings
- Read and write files
- Modify registry settings
- Automate computer maintenance
- Automate remediation of problems detected via monitor
- Automate the updating of third party applications

Once established, scripts can be scheduled to run:

- According to a schedule
- On-demand
- As part of a monitor detection process

Plan and implement scripts to complement your technology solution contracts since the script functions are the most commonly used automation tool and extremely powerful.

Monitors – Internal and Remote

ConnectWise Automate monitors are used to monitor the condition of any device and then perform an action (i.e. raise alert, open a ticket, send email, execute a script, etc.) when a threshold is reached. There are two classes of monitors in ConnectWise Automate: internal and remote. Internal monitors are operated from the ConnectWise Automate server through SQL statements and database queries. Remote monitors are the system and network monitors that run external from the ConnectWise Automate server on an agent-enabled computer.

Internal monitors are system friendly in that they are displaying information that is stored in the ConnectWise Automate database and are therefore not agent intrusive. The disadvantage to using this sort of monitor is that
the information available is controlled by the agent schedule and may not be up-to-the-minute. Almost all alerting options are applied at the group level for internal monitors to allow per group monitor mapping in the PSA plug-in and to allow varied alerting based on the selected service plan.

Note: Exception monitors that are not related directly to an agent, such as client or location monitors, are applied globally.

Remote monitors are very useful for gathering up-to-the-minute system information due to the following:

- Remote monitors run on the local agent and can check the agent in real-time, alerting faster in case of a failure
- Remote monitors are incredibly scalable
- Leverage the agent’s processing
- Low impact on the agent CPU/RAM
- Zero impact on bandwidth or server storage
  - Remote monitors only trigger on fail/success status change

Some Cautions to Exercise with Remote Monitors are as Follows:

- Do not randomly set remote monitors as data collectors
- An executable run by a remote agent runs under the same user that the agent service is running under, which is normally the local system account
  - This limits remote monitors from querying Active Directory services like Exchange, unless you have set your agent to run as a user that has these permissions
Patch Installation Windows

Patch installation windows are defined by the patch specific templates and define the scheduled patch installation day and time, as well as the schedule patch reboot window if applicable. One key thing to note about patch install windows is they do not assign patches to be installed; rather they simply configure the managed machine for the time to apply what is approved in advance.

The following configurations for patch installation are deployed with ConnectWise Automate Ignite:

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Template Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do Not Patch</td>
<td>The ‘Do Not Patch’ template is associated with the ‘Patch Control-Do Not Patch’ grayed out master group. Any clients that you do NOT want to approve updates on should be dragged to this group. This template will do nothing with Windows Updates. All other settings are not enabled.</td>
</tr>
<tr>
<td>Windows Updates Servers: – Everyday</td>
<td>The ‘Windows Updates Servers - Everyday’ template is associated with the ‘Windows Updates Servers - Everyday’ master group. Servers that meet the corresponding search and are added to the ConnectWise Automate system will automatically be placed in this group. This template is configured to use the schedule for inventory only, use ConnectWise Automate mode for Windows Updates and the hotfix install/reboot window is set for 2am. All other settings are not enabled.</td>
</tr>
<tr>
<td>Windows Updates Servers: Monday – Friday</td>
<td>The ‘Windows Updates Servers - Monday’ template is associated with the ‘Windows Updates Servers - Monday’ master group. Servers that meet the corresponding search and are added to the ConnectWise Automate system will automatically be placed in this group. This template is configured to use the schedule for inventory only, use ConnectWise Automate mode for Windows Updates, hotfix install window set to 2am and hotfix reboot window is set for everyday at 2am. All other settings are not enabled. Each of the subsequent day templates are the same except for the hotfix install window day will correspond with the template name.</td>
</tr>
</tbody>
</table>
Handle Alerts/Tickets That Are Generated From ConnectWise Automate

Being able to automatically generate and manage service tickets in your professional services automation (PSA) software based on real-time alerts in your RMM software allows you to respond quickly to customer needs. But why should you ticket everything that is generated from the RMM software? This is a highly debated topic, but in reality it comes down to the single idea of “information.” Creating these tickets provides a full-sized stream of information about your clients’ machines and networks and can be used to show root causes for some problems, predict new problems before they occur and simplify troubleshooting for your technicians.

Learning to manage these alerts and separate the more important items from the less important ones is critical to being able to provide an acceptable level of client service and satisfaction. As you develop your overall ticket strategy, keep in mind that the overarching goal is to maintain details to help in justifying your service delivery, as well as to help a technician pinpoint trouble in an efficient and quick manner.

Consider the following example and how the capturing of installed software could potentially reduce problem resolution time. Your customer has installed an “Office Add-In” for Microsoft Word and your RMM system detected the change as newly installed software and reported it via a ticket that was automatically generated. A few days later the client contacts your service desk and opens an incident related to Word crashing repeatedly. Your technician is trained to begin the logical process of troubleshooting within the service ticket area of your PSA and within minutes the tech finds the offending application that was installed by the client a few days earlier and removes it with your RMM tool. He alerts the customer and asks that they watch the issue and let him know if it occurs again and advises that the likely cause was the add-in that was installed and advises against re-installing the add-in or any future add-ins.

Now consider a scenario in which the software installation wasn’t being monitored and ticketed. The same event occurs, but instead of resolving it quickly, the technician begins troubleshooting. The tech is blind to what transpired and spends countless hours searching for the issue. It’s like trying to find a needle in a hay stack. Since the add-in did not register in Add/Remove Programs, the technician never finds that it was user installed and the likely culprit. Therefore, the tech cannot effectively resolve the situation. Is this situation extreme? Yes, but it certainly builds a strong case for ticketing all events as they are detected.

Managing Ticket Generation

Listed below are some key areas of management that the technology solution provider should focus on to better manage ticket generation that produces alerts that overlap from different clients being managed by the RMM solution.

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Template Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Updates Workstations: – Everyday</td>
<td>Same as Windows Updates Servers – Everyday but for servers.</td>
</tr>
<tr>
<td>Windows Updates Workstations: Monday – Friday</td>
<td>Same as Windows Updates Servers: Monday – Friday but for workstations.</td>
</tr>
</tbody>
</table>
• On-Boarding: Use care when on-boarding new clients so that a methodical approach is applied to help better manage overall ticket creation
• Understand It: Why is this important to my business?
• Manage: Tune your system for what is acceptable
• Adjust monitor conditions where required
• Software install
  » Blacklisted software
  » Event blacklist
  » Services blacklist
  » Process list
• Use Exclusions: Exclude machines where required
• Consolidate: Consolidate tickets when possible via scripts
• Workflow: Use PSA workflow to auto close tickets that are not of high importance when techs cannot turn them around fast enough (72 hour close is a good starting point)

**Top Ticket Generating Monitors and Monitor Types**

The chart on the following pages represents the 10 highest ticket producers from ConnectWise Automate and explains why these are important, where they come from and how to better manage them to provide valid information versus noise in your PSA system. While this list is not all-inclusive, it was generated from support requests into the ConnectWise Automate help desk following the rollout of ConnectWise Automate Ignite and generally shows the top issues as reported.

<table>
<thead>
<tr>
<th>Monitor or Type</th>
<th>What It Does</th>
<th>Why Is It Important</th>
<th>How Do I Manage This</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectWise Automate – No Agent Checking In (30 Days)</td>
<td>This alert notifies you of any machine that has not checked into the ConnectWise Automate server for 30 days.</td>
<td>The assumption here is that you are providing a monthly service to your clients and if a machine has not reported in within the month, you could not perform what is required of you to deliver your service.</td>
<td>Exclude at monitor level specific machines that can be ignored or contact clients to determine why a contract device isn’t powered on.</td>
</tr>
<tr>
<td>Monitor or Type</td>
<td>What It Does</td>
<td>Why Is It Important</td>
<td>How Do I Manage This</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change Management Tickets</td>
<td>Upon on-boarding and each day, servers are checked for roles and or changes to roles and tickets are generated with the detail.</td>
<td>Not all TSPs are in full control of their clients’ environments. This process is designed to keep you up to speed on changes you may not be aware of and validate whether stuff you should be aware of was completed if requested.</td>
<td>Workflow within your PSA is your best solution here so you maintain the history of changes. SP1 will introduce ticket management for tickets like this to close them automatically after X days if they have not been reviewed.</td>
</tr>
<tr>
<td>ConnectWise Automate Onboarding/</td>
<td>The monitors alert you to issues that should have been addressed within ConnectWise Automate during location on-boarding by a technician.</td>
<td>This will ensure that all of the required steps are complete and you get the desired action you expect out of the system.</td>
<td>Complete the required tasks to effectively on-board each client by replacing the Not Selected Default value in the service plans with something that is appropriate. Ensure patch day assignments are completed if patching is enabled and make sure each location has admin credentials in ConnectWise Automate.</td>
</tr>
<tr>
<td>Patching</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance Monitors</td>
<td>These monitors monitor specific performance variables on workstations and servers, as well as by server roles.</td>
<td>All performance monitors that are set to trigger are based on Microsoft’s published best practices, so if something is alerting, it exceeds the published threshold and should be investigated.</td>
<td>Each of these alerts that doesn't auto reset after the threshold is lowered should be investigated and remediated. In addition, any alerts that show a pattern of reoccurring even if they reset should be investigated as both situations represent an issue based on performance.</td>
</tr>
<tr>
<td>Monitor or Type</td>
<td>What It Does</td>
<td>Why Is It Important</td>
<td>How Do I Manage This</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sensor Monitors</td>
<td>These monitors monitor specific motherboard sensors for conditions that are excessive.</td>
<td>This is one area where partners are not doing justice when it comes to monitoring machines and can indicate possible failures prior to disaster striking.</td>
<td>Sensors are set to alert after the third failure and will auto close if a condition clears. Management is via properties within ConnectWise Automate if you think the default values do not fit your environment. These can also be overridden at the machine level if the need arises.</td>
</tr>
<tr>
<td>EV – Blacklisted Events</td>
<td>Currently three monitors monitor the blacklist event table for alerts that match entries within the table. They are Critical and Warning Events, Exchange Events and Informational Events that all match the list.</td>
<td>The events are listed within the blacklist by specific ID or message, as well as source, and indicate true issues that need to be investigated and remediated.</td>
<td>If an event is on the blacklist that you feel should not be, simply remove it from the list and no more alerts on that event will be generated. This list can also be used to add application specific events for clients’ applications if the need exists. The real thing with this type of alerting is fix the issue at hand and the alert will stop.</td>
</tr>
<tr>
<td>Monitor or Type</td>
<td>What It Does</td>
<td>Why Is It Important</td>
<td>How Do I Manage This</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SW – Uninstalled</td>
<td>This monitor looks for applications that have been removed from computers but excludes common apps such as Java, Adobe, etc. that frequently do a removal when they are updated.</td>
<td>How can you tell if a business line app or some management tool was removed by mistake without monitoring this? This also creates a ticket which serves as a record if a customer has requested something be uninstalled and will validate that you completed the requested task for them.</td>
<td>This monitor already consolidates tickets for each machine, so you are not notified via more than one ticket per machine if stuff was removed. If you need to exclude a machine, that can be done via the exclusion tab.</td>
</tr>
<tr>
<td>SW – Installed New</td>
<td>This monitor looks for applications that have been added to computers, but excludes common apps such as Java, Adobe etc. that are common and updated often.</td>
<td>Potential harmful applications that threaten your network security can be installed by users, such as file sharing apps and backdoors.</td>
<td>This monitor already consolidates tickets for each machine so you are not notified via more than one ticket per machine if stuff was added. If you need to exclude a machine, that can be done via the exclusion tab.</td>
</tr>
<tr>
<td>SW – Unclassified Apps</td>
<td>This monitor looks for applications that have been installed at some point on the various machines and lets you either whitelist or blacklist the application as either known good or bad.</td>
<td>Potential harmful applications that threaten your network security can be installed by users and this process lets you mark them by classification and then lockdown the known bad ones and alert on them.</td>
<td>This monitor already consolidates tickets for each machine so you are not notified via more than one ticket per machine if stuff was added. If you need to exclude a machine, that can be done via the exclusion tab. You also should manage the Application Whitelist within ConnectWise Automate to further manage these alerts, as listed apps will no longer generate tickets as they are located.</td>
</tr>
<tr>
<td>Monitor or Type</td>
<td>What It Does</td>
<td>Why Is It Important</td>
<td>How Do I Manage This</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SVC – Auto Services Stopped</td>
<td>This monitor runs each hour looking for services that are reported stopped, but set to an automatic start state.</td>
<td>This is important since many line of business applications are service driven and it keeps you from having to identify each and every service that needs to be running. It runs a script to restart the stopped service, does multiple passes and then reports on success.</td>
<td>The additional services that are set to auto by the application installer but really only start when the app is launched can be excluded by adding them to the Auto Services Blacklist. This is done by either manually adding the items to the table located under dashboard/configuration/config or by right-clicking on a service in the service tab and adding it to the blacklist. If you need to exclude a machine, that can be done via the exclusion tab.</td>
</tr>
</tbody>
</table>

**System Tuning and Adjusting**

Several areas within ConnectWise Automate will help you manage tickets over the long haul. By establishing policies within your organization around these areas of the system and by maintaining them on a routine basis, an TSP can easily manage the flow of the more common tickets and cut down on the overall ticket creation. Each of the following areas represent areas that Automate Administrators should be trained to manage on a regular basis.

**Application Whitelist Management**

The Application Whitelist screen displays all of the applications that have been whitelisted because they have been approved for use by ConnectWise Automate or a technician. By default, thousands of applications have been added to the whitelist for your convenience.

This will not prevent an application from being installed; however, if an application is installed that does not appear on the application whitelist or blacklist, it will cause the ‘SW-Unclassified Apps’ monitor to alert you of an unclassified application so you can determine if the application is safe and should be approved. Please note that by default, this monitor is only installed on managed groups.

Whitelisted applications will appear normally on the Software tab of the Computer Management screen. Any applications that have not been classified will display in bold and any blacklisted applications will display in red.
To access the Application Whitelist screen:

From the Control Center, select Dashboard>Config>Configurations>AppWhitelist.

**App Whitelist Screen**

Programs that have been deemed safe or suitable can be added to the application whitelist.

To add programs to the application whitelist:

Enter the name of the program into the Name field. The name should be entered the same way that it would appear in the Add/Remove Programs list within the Control Panel of Microsoft Windows.

**NOTE:** Applications can also be added to the whitelist from the Software tab of the Computer Management screen by right-clicking on the application and selecting Software > Add to Whitelist.

**Event Blacklist**

The event blacklist is a list of events that have been specified to be monitored by the ConnectWise Automate system. This is useful when there is a specific event that indicates a potential security risk or critical system failure.
To access the Event Blacklist screen:

From the Control Center, select Dashboard > Config > Configurations > Event Blacklist.

**Event Blacklist Screen**

To add an event log to the event log blacklist:

1. Enter the event log’s Event ID, Source, Message, Log Name, Event Type, and Category into the respective fields
2. Click Add

To modify a log in the event log blacklist:

1. Select an event log from the list of events blacklisted; the information for the event log should automatically populate in the fields at the top of the screen
2. Make the desired changes and click Save
To delete an event log from the blacklist:

1. Right-click on event log and select Delete; you will be prompted if you want to delete the event log
2. Select Yes to delete the event log from the blacklist or No to close the window and cancel the operation

**Services List**

Blacklisting services allows you to prevent specific services from raising alerts when the service is stopped. For example, if you have a monitor that checks for auto-start services that are running and an auto-start service that has been added to the blacklist has been stopped, an alert will not be raised.

Services can be blacklisted from the Services tab of the Computer Management screen or they can be added to the master list in the Dashboard (Dashboard > Config > Configurations > Services Blacklist).

The Service Blacklist screen allows you to add different services to the blacklist and prevent them from raising alerts when they are stopped.

To access the Service Blacklist screen:

From the Control Center, select Dashboard > Config > Configurations > Service Blacklist.

**Service Blacklist Screen**
Services can be added to the blacklist from the Services tab of the Computer Management screen or in the Dashboard.

To add services to the blacklist from the Computer Management Screen:

1. From the Control Center, expand Clients > Client > Location and double-click on an agent machine
2. Select the Services tab

**Services Tab**

1. Select the desired service(s) from the list; you can select multiple services by holding down the [Shift] key or by using the [Ctrl] key
2. Right-click and select Blacklist Service from the menu; the list will immediately update and the blacklisted service(s) will be highlighted in pink

**NOTE:** Blacklisting a service in the Services tab of the Computer Management screen will automatically add the service to the Service Blacklist screen in the Dashboard.

To add services to the blacklist from the Dashboard:

1. From the Control Center, expand Clients > Client > Location and double-click on an agent machine
2. Select the Services tab
3. Select the desired service(s) from the list; you can select multiple services by holding down the [Shift] key or by using the [Ctrl] key
4. Right-click and select Blacklist Service from the menu; the list will immediately update and the blacklisted service(s) will be highlighted in pink

**NOTE:** Blacklisting a service in the Services tab of the Computer Management screen will automatically add the service to the Service Blacklist screen in the Dashboard.
1. From the Control Center, select Dashboard > Config > Configurations > Service Blacklist

2. Enter the name of the service as it would appear in the Services tab of the Windows Task Manager in the Name field (e.g., WdiServiceHost)

3. Enter a display name for the service in the Display Name field (e.g., Diagnostic Service Host)

4. Enter a description of the service into the Description field (e.g., Performs problem detection, troubleshooting and resolution for Windows components)

5. Select the Enforce checkbox to enable blacklisting of the service

6. Click the Add button to add the blacklisted service; the list will immediately update with the new entry

To modify a service on the Service Blacklist screen:

1. Select a service from the list; the information for the selected service will automatically populate in the fields

2. Make the desired changes to the entry; note that the Add button will change to a Save button

3. Click the Save button; the list will be updated with the saved changes

To delete services from the blacklist on the Computer Management Screen:

1. From the Control Center, expand Clients > Client > Location and double-click on an agent machine

2. Select the Services tab

3. Select the desired service(s) from the list; you can select multiple services by holding down the [Shift] key or by using the [Ctrl] key

4. Right-click and select Remove Blacklisted Service from the menu; the service(s) will no longer be blacklisted and the pink highlighting will be removed

To delete services from the blacklist from the Dashboard:

1. From the Control Center, select Dashboard > Config > Configurations > Service Blacklist

2. Select the desired service(s) from the list; you can select multiple services by holding down the [Shift] key or by using the [Ctrl] key

3. Right-click and select Delete from the menu

4. A prompt will appear asking you to confirm; click Yes to delete the services; the services will be immediately removed from the list

**Process List**

The Process List screen is used for informational purposes to allow you to compare processes running on an agent to determine if a process that is running is known to be a virus, spyware, etc. For your convenience, ConnectWise Automate has classified thousands of processes as spyware, viruses, grayware and normal by default. Additional processes can be added and classified, as necessary.

The Process List will not prevent a process from running; however, if a process is detected as a virus/spyware,
it will cause the ‘NC – Bad Processes Detected’ monitor to alert you of a bad process. Please note that this monitor may only be installed on specific groups.

To access the Process List screen:

From the Control Center, select Dashboard > Config > Configurations > Process List

**Process List Screen**

To add a process to the process list:

1. Enter the Friendly Name of the process in the process list
2. Enter the Process Name for the process (this is the specific name used by Windows for the process)
3. Select the process classification from the Status drop-down; the available options are Virus\Spyware, Good Program and Grayware
4. Enter the executable name of the process in the Executable field
5. Enter a description of the process in the Description field
6. Click the Add button; the entry will be immediately added to the list

To modify a process in the process list:

1. Select a process to modify from the list of processes; the information for that process should automatically populate in the fields at the top of the screen
2. Make the desired changes to the entry; note that the Add button has changed to a Save button
3. Click Save; the list will be immediately updated with the saved changes

Exclusions – Group Created Monitor Overrides

If the monitor is created from a group, the box at the bottom will show (Group Created Monitor) and indicate the group that created the monitor. It will also give you an override checkbox. If you check this box, the monitor can be edited here and it will remain and the group will not change it back to the original configuration. In this case, the monitor is still attached to the group, so if you remove the computer from the group, it will then remove this monitor from the computer, even if its override is checked. If the override is unchecked later, it will auto sync the monitor next time it syncs and replace the group settings back onto the monitor as they are currently defined.

When you have the override checked, you can change ANYTHING, including the NAME of the monitor and those changes override whatever the group initially set for the monitor.

Machine Monitor with Override Set
Consolidation – Handling Duplicate Tickets

Even after you have tuned your ConnectWise Automate installation to filter out known good software, services and processes from alerting, there are still certain types of monitor alerts that are repetitive by nature. Good examples of this are event logs, smart drive errors and failed logins. In the past, each monitor alert would create a new ticket for each monitor event that was triggered and that would pile up tickets that were repetitive in nature over time. Ticket consolidation scripts are the solution to reduce the number of tickets generated in these instances.

A ticket consolidation script creates a single ticket for a specific type of monitor alert on a computer and adds an additional ticket comment for each additional alert to the same ticket, while the ticket is open. An example of this would be critical blacklisted event log entries for a single computer. If more than one alert is sent by the monitor, the additional alerts will be added to the open ticket until the ticket is closed. Having all related event log entries on a single ticket allows you to put them in context and identify recurring problems to be addressed.

This example shows Critical Blacklisted Events for a single agent.

In ConnectWise Automate Ignite, ticket consolidation scripts are simplified to empower easier creation of new ticket consolidation scripts. All ticket logic is removed to a subscript, leaving only the ticket text defined in the header of the script. This allows the text generated by the script to be easily reviewed or modified. The script can be copied as a template and a new ticket consolidation script can be created based on the original script.

In the Monitor SW Install scripts, lines 3-6 define the text that will be used to create and append the ticket created by the script.
Ticket Consolidation Workflow

1. An internal monitor alerts, triggering an alert that calls the Alert Template that is defined on the monitor.

2. The Alert Template can have several types of alerts related to it. In order to call a ticket consolidation script, you must select the alert action of script and select the name of the ticket consolidation script to run.

3. The ticket consolidation as shown above handles the text to be used in the generated ticket and calls the main ticket consolidation subscript.

When Tickets Overflow

One concern with ticket consolidation is that if left unchecked and the monitor is generating large numbers of alerts, the consolidated ticket can grow very large with each alert adding a new comment to the existing ticket. As the ticket grows larger, editing those tickets becomes unworkable.

ConnectWise Automate Ignite established a system property that defaults to a maximum of 50 ticket comments appended to any ticket consolidation script to control the growth of tickets. This value can be changed, but once the defined maximum number of comments has been appended to a ticket, a comment will be added to the ticket that states, “Max Ticket Comments Reached: No more script generated comments will be appended to this ticket to stop the ticket from growing to an unmanageable size. Further monitor alerts for this issue will be dropped while this ticket remains open.” Any further monitor alerts will be dropped for this issue. This limits the size that a ticket can grow to, but does lose information that should be tracked.

Workflow – Manage Information via PSA Tool

Most technology solution companies have a service ticketing workflow that is critical to company success. How you manage this process can make or break your business. Clients judge you on your capability to efficiently capture service issues from multiple sources, the speed with which you respond and the quality of
the service work you provide. Coupled with the clients' expectations is our inherent need to store information and be able to report on it at a later time from a historical perspective or for troubleshooting.

Using professional service automation software workflows will make managing your service tickets and tasks easier. There are three basic types of workflow to focus on for service delivery: status workflow, escalation workflow and auto resolution workflow.

**Service Ticket Status Workflows**

- Define notifications (internal and external) to be executed when a service ticket is changed to a specific status
  - Use multiple steps for service statuses where applicable
  - Update the customer on status changes when appropriate

**Service Ticket Escalation Workflows**

- Define steps to be executed based on conditions (triggers) for a service ticket.
  - Use multiple actions in your triggers if needed such as change status, re-assign ticket or move service board location
- Auto assign high priority tickets to the correct service team or resource
  - Server down conditions
  - Site down condition
  - Critical service outage

**Service Ticket Auto-Resolution Workflows**

- Define auto closure timeframes for alerts that are informational or historical in nature to keep tickets from piling up; a 72 hour timeframe is a great starting point
DOCUMENTING THE VALUE OF YOUR AUTOMATION

It is important that as a technology solution provider, you continually document the value of the service that you are providing to your clients. If this is not done, your clients will see your service as a cost center rather than a critical investment in their business. You are likely already promoting major features of your service, such as backup and disaster recovery or security solutions that give your client peace of mind that their IT needs are handled. You should also be featuring your employees as they are probably your firm’s largest investment. Let your clients know about your employees, their capabilities, certifications and just a little about them that humanizes them to your clients, so they are not just a voice at the end of a phone call or someone closing a ticket. Your goal is to become their trusted advisor and complete provider of all things IT for their business. You need to let them know you have invested in the right solutions and team to successfully support their IT needs.
Your investment in automation is another thing that you should place front and center in your client communications. You have made significant investments in the tools to support your TSP practice. When they are leveraged properly those investments are a competitive advantage for your firm. Your clients do not care that you have purchased Manage or Automate. In fact, those brands should never be communicated to your clients. The point to make to your clients is that your firm is always thinking about ways it can efficiently improve their IT environments. Automation where possible is a key piece of each of those solutions.

Your clients are concerned about how you can reliably support their business and improve their productivity. If you can say to them that we proactively monitor for low disk space on their servers and workstations and will automatically free wasted drive space to avoid system outages, this is much better than a firm that responds reactively to servers with full hard drives and an office of employees standing around unproductive. Since your solution is automated, it is better than the most diligent technician or your client’s part time IT employee. Your automation checks for these conditions every five minutes, catching a drive rapidly filling with Exchange log files before mail stops flowing on that server. Without automation, that level of diligence is impossible.

ConnectWise Automate Ignite provides two main methods to document your automation in the form of tickets related to different automation performed.

**AutoFix Time:** Any autofix script can be enabled to post time to generated tickets. This includes service restarts, killing bad processes, disk defragmentation and disk clean up.

**Patch Accounting:** The patch accounting option in ConnectWise Automate Ignite will create tickets for all successful patch install jobs completed in the past 24 hours. You can optionally enable time based on the actual time it took to install the patch or specify a flat rate per successful patch job.

You can also use third party solutions such as App-Care or Ninite scripts to document updates of third party applications. Any script you modify or build can be set to create tickets, add comments and optionally post time using ConnectWise Automate script ticketing functions or the script’s Script Time tab.

**Configuring Autofix Time**

Autofix time is enabled globally using Ignite System properties in Dashboard > Config > Configuration > Properties

- `_sysTicketDefaultMinutesToBill` – The default number of minutes to bill for each autofix.
- `_sysTicketDefaultTimeCategoryID` – The default time category for the time to be posted. The Time Category ID can be pulled from the Dashboard > Config > Configuration > Time Category.
• _sysTicketUserID – The default ConnectWise Automate UserID to post time on tickets. The UserIDs can be pulled from the Nav Tree Admin > Users and open the User you wish to use. The UserID will be in the window title. The spelling of this ConnectWise Automate User must match a corresponding Manage member for time to post properly.

• _sysTicketEnableAutofixTime – Enables (1) or Disables (0-Default) posting time for autofixes.

The default time set in the _sysTicketDefaultMinutesToBill property can be overridden for individual scripts by editing the individual script and modifying the Minutes value under the Time Recording tab. The settings edited here are not saved with the script, so updates of the script logic will not override changes you make on the Time Recording tab. The values beginning with @prop are the values of the properties listed above.

Configuring Patch Accounting

Patch accounting is enabled globally using Ignite System properties in Dashboard > Config > Configuration > Properties.

_sysPatchAcctTicketJobSuccess – Enables (1) or Disables (0-Default) posting time for patch install jobs.

_sysPatchAcctTimeToBill – Leaving the property set to (0) disables patch accounting. Setting (1) enables billing based on the actual install time of the patch job. Any value greater than 1 is billed as the flat number of minutes to bill for each successful patch install job.

Patch accounting runs once a day at 6 a.m. by default and only looks at patch install jobs that have completed in the past 24 hours. The ticket process will never leave a ticket in an open state, as there is no remediation that is run during patch accounting. If there is a successful patch install job, a ticket is created, time is posted and the ticket is closed. If there are any failures in the patch install job, the whole job is considered failed.

How to Handle All of This Automated Ticket Time

ConnectWise Automate takes care of creating the tickets and posting the time, the PSA plug-in in ConnectWise Automate handles synchronizing the tickets over to PSA software. Once the tickets and time have synced, the real question becomes what to do with the time and how to handle the time on PSA software.
customer agreements. The solution that needs to be implemented is that clients with proactive automation work time should have the time included as part of their agreement whereas non-proactive clients should have the time billed or you should not be providing automated service to the client.

Prior to ConnectWise Automate, all ConnectWise Automate script generated tickets were sent to a single Manage service board. This limited the solution to defining a default work type on the Manage service board, such that as new work time was posted onto the defined scripts board, the time took the board’s default work type. Then that work type could be included or excluded from different agreement types.

In ConnectWise Automate, the concept of ticket categories provides multiple options to tag tickets generated by monitors or directly by scripts to different ticket categories. The ConnectWise Manage can then map different ticket categories to different Manage service boards and service types or to specific service types, sub types and items if you are using ITIL. As you are able to define the service type more specifically, you are able to define more service types and specify multiple types of automation that are included or excluded from your service plan agreements. The entire concept of ticket category is designed to allow TSPs to easily define service boards for large types of tickets for better management. Simply put, if you want all of the performance monitors assigned to a single board, it can be accomplished by setting all performance monitors to a specific ticket category and then assigning that category to a service board with a priority and service type. If then, the service type that was assigned is excluded from your contract agreement billing, the tickets will be created and flow to your detailed invoicing at a zero dollar charge and build overall value in what you do for your client.

Defining @TicketCreationCategory@ for Scripts

The Script Create Ticket function looks for a user script variable @TicketCreationCategory@=X where X is the Ticket Category ID to be set. Ticket categories can be set in scripts in three different ways.

1. If the script is an auto-fix script that is being called from a monitor or an alert template, the @TicketCreationCategory@ variable will be set from the Ticket Category set on the originating monitor and passed through to the autofix script.

2. You can set the @TicketCreationCategory@ variable any place in a ConnectWise Automate script as long as it is before the Ticket Create function is called.
3. You can pass the `@TicketCreationCategory@` value as a parameter to a script scheduled against a group. If there is more than one parameter passed to a script, parameters must be separated by the pipe symbol in the format “TicketCategory=108|param2=X|param3=y”.

---

Do Not Hide YOur Automation

It is important that you are upfront with your clients about your automation. Attempting to position that your third shift employees are very efficient will not hold water for long; thus, it is recommended you simply specify that automation is a piece of the total solution your firm brings to its clients. When setting up time billing for automated tasks, it is always best to bill for less time than it would take any technician to accomplish the same task. If you are challenged that automation is accomplishing large amounts of your service, confirm this and add that you have invested heavily in both time and money to build the solution. If the client still holds the position that there is no value to the automation, you can stand on the position that your automation accomplishes the task in less time than any person working in front of the computer and since it works silently in the background, often after hours, there is much less impact to their employees’ productivity.

From a business perspective, if you analyze the time that is recorded on average due to work that your automation system is producing, you will see the true value that it presents your company. Routinely, technology solution providers that invest in building out automated processes will see a weekly bill average for the automation system in the 40 to 100 hour range if they support 1,000 or so endpoints. If we break that down into FTE units, that means our automation system accounts for one to two and a half full-time employees, but it is at a fixed cost and isn’t sick, on vacation or in need of a break – it just performs. To make your offering and business a success, you must invest in building out automated processes for service delivery.
BEST PRACTICES FOR WINDOWS PATCH MANAGEMENT AND INSTALL

By understanding the different kinds of patches and following a simple regime, a technology solution provider can keep clients’ critical systems free from known vulnerabilities.

Patch management is probably the biggest concern of TSPs and their clients these days. With new vulnerabilities being discovered almost weekly, keeping systems up-to-date with patches is often a full-time job, especially in larger environments. In addition, the lag time between when a vulnerability is discovered and when a virus or worm appears in the wild is now measured in days or weeks rather than months. This
puts tremendous pressure on vendors to release patches before they've even been fully regression-tested. The result is that sometimes, patches fix the problem they're designed to address, but break something else unintentionally in the process. Customers and partners often blame vendors in such circumstances but, let's face it, there's a war going on and like most wars, it's messy.

Most TSPs pay attention to security and patching their clients' systems, but how many have a well-honed patch management policy? Patch management is often seen as a trivial task. Simply click on 'update' and that's it. But in reality, there is a lot more to it and a proper policy is certainly not overkill. But what should a patch management policy include apart from deploying patches?

Patch Flavors

Before you plan a patch-management strategy, it's important to understand the differences between the various different flavors of patches. Microsoft classifies patches into three basic categories: hotfixes, roll-ups and service packs.

Hotfixes

Hotfixes are small patches designed to fix a single problem and are developed either in response to a security advisory or by customer request. Hotfixes are typically issued either to plug security holes, such as buffer overflows, or to fix features that don't behave as intended. Not all patches are created equal; hotfixes that address broken functionality are developed by Quick Fix Engineering (QFE) teams at Microsoft Product Support Services (PSS), whereas those that address security vulnerabilities are identified and developed by the Microsoft Security Resource Center (MSRC).

Roll-Ups

Occasionally, Microsoft combines several hotfixes together into a single package called a roll-up. This is typically done when several security issues have been identified within a short time interval and its purpose is to simplify the job of installing hotfixes for administrators. Unfortunately, this is not always a good idea. There have been instances in which installing multiple patches broke applications, and the headache then arises: figuring out which patch in the roll-up actually caused the problem.

Service Packs

At fairly regular intervals, Microsoft combines all hotfixes issued for a platform into a single package called a service pack. These service packs are cumulative. For instance, Service Pack 3 includes all hotfixes issued both before and since Service Pack 2 appeared. While service packs undergo more thorough testing than individual hotfixes, there have nevertheless been a few instances in which a service pack caused new problems while solving others.

MSRC Ratings System

Hotfixes that address security vulnerabilities are also called security fixes and the MSRC rates these according to a four-point scale from high to low. This is a useful scheme for administrators, because it allows them to decide which fixes should be applied as soon as possible and which can be deferred until later or even ignored. The ratings also refer to the types of vulnerabilities they guard against. An example of a critical issue
might be a self-propagating Internet worm that can bring servers to their knees and wreak other kinds of havoc, while important means that your confidential business information might be at risk of being lost, stolen or corrupted. Moderate means you have a properly configured firewall and are following good security practices, so you aren’t likely to be affected by this problem, though it’s still possible. Finally, low means it would take a combination of a genius hacker and a totally negligent system administrator for this exploit to occur (but it’s still remotely possible).

**PATCH POLICY BEST PRACTICES**

Effective patch management can be summarized as policy, process and persistence (PPP). Let me unravel this, along with some helpful recommendations from Microsoft.

**Policy**

The first step in developing a patch management strategy is to develop a policy that outlines the who, what, how, when and why of patching your systems. That takes planning on the TSP’s part, and with administrators being as busy as they are these days, it’s difficult to allocate time for proper planning. Still, planning is essential. My view is that the difference between planning and an ad hoc fix-it-when-it’s-broken approach is the difference between peace of mind and success, and constant anxiety and a disaster waiting to happen.

It all boils down to being proactive instead of reactive. Proactive management anticipates problems in advance and develops policies to deal with them; reactive management adds layer upon layer of hastily thought-up solutions patched together using bits of string and glue. It’s easy to see which approach will unravel in the event of a crisis. Once you have a patch management policy in place (usually it’s part of your overall security policy) and a notification arrives of a critical vulnerability in some product, you immediately know who will deal with it, how you will deploy the patch, whether it needs to be done sooner or later, and so on. For example, a simple element of a patch management policy might be that critical or important patches should be applied immediately, while moderate or low patches should be submitted to a team member for further study. Another example is proactively scheduling a specific day of the week or month for installing patches (usually weekends, in case something breaks), as opposed to the drop-everything, the-sky-is-falling approach common in a reactive environment. Making a decision tree that addresses these issues ahead of time reduces anxiety and speeds response when the time comes to patch something.
Process

The detailed procedure you will use to respond to vulnerabilities and deploy patches should be explicit within your security policy. The typical patch management process is illustrated below by the process workflow in general terms and includes aspects of ITIL to ensure success.

**Typical Patch Management Process**

The following six-step process is defined as best practice by Microsoft and should also be considered as you craft your own tailor made process for use within your technology solution practice.

1. **Notification**

   Information comes to you about a vulnerability, including a patch meant to eliminate it. Notification might be sent via email from the Microsoft Security Notification Service, a pop-up balloon when you’re using Automatic Updates, a message displayed in the Software Update Services (SUS) web console, or some other method. It all depends on which tools you use to keep your systems patched and up-to-date.

2. **Assessment**

   Based on the patch rating and the configuration of your systems, you need to decide which systems need the patch and how quickly they need to be patched to prevent an exploit. Obviously, having an accurate inventory of systems and applications running on your clients’ networks is essential if you want to keep the networks secure against intrusion.

3. **Obtainment**

   How you get the patch you need depends on which patch management tools you choose to deploy. In general, such tools range from completely manual (i.e. visiting the Windows Update website) to almost entirely automatic (i.e. via Automatic Updates, ConnectWise Automate or SUS). Like everything in security, there is a tradeoff: the manual approach is slower, but it gives you more control.

4. **Testing**

   Testing should always take place before you apply patches to production systems. Test your patches on a test bed network that simulates your production network. Remember that Microsoft can’t test all possible effects.
of a patch before releasing it, because there are thousands of applications that can run on servers and millions of combinations of applications. Thus, make sure you test patches before deploying them, especially if you have custom code running on your machines. If you need a way to justify the cost of purchasing duplicate equipment for a test bed network, tell the boss it’s like insurance. This is one area that most TSPs that are small in size tend to overlook due to equipment and time constraints, but in reality they are the ones that should really keep an eye on patch testing. Think of it this way, if you deploy patches to a client that has 15 systems and you wreck them all at once, that client is effectively out of business until you get everything restored – the risk of blowing them up is directly related to the likelihood that they will keep you as their provider following the restoration. If you can’t afford to lose a client, you need to plan for some level of patch testing.

5. Deployment

Deploy a patch only after you’ve thoroughly tested it. You are then ready to apply it, but do so carefully. Don’t apply it to all your systems at once, just in case your testing process missed something. A good approach is to apply patches one at a time, testing your production servers after each patch is applied to make sure applications still function properly. That’s the problem with security roll-ups: by combining several fixes into a single package, the probability of a patch going wrong and breaking something is multiplied. Again, it’s a tradeoff: roll-ups speed up patch deployment, but give you less control over the result. A major consideration to deploying should also be based on geographic location. If you have a client with three locations, you should probably be applying patches on three separate days for this client to avoid a situation where you potentially take out the entire company if one patch has an issue following deployment. It is certainly better to be safe than sorry in this case and the little extra care will go a long way with client relations if something negative were to come from the patch cycle.

6. Validation

This final step in the process is often forgotten: making sure that the patch has actually been installed on the targeted systems. The validation process must be completed so that when it comes time to report on status to your client, you are certain that the data being submitted is an accurate representation of the actual patch status. This reporting and validation process takes some time, but is a very necessary procedure to ensure that service levels are met.
Persistence

Policies are useless and processes are futile unless you persist in applying them consistently. Network security requires constant vigilance, not only because of the new vulnerabilities and patches that appear almost daily, but because new processes and tools are constantly being developed to handle the growing problem of keeping systems patched.

So, we are on the horns of a dilemma. If you assert that Microsoft is responsible for ensuring that Windows systems are patched and up-to-date, then you should agree that Microsoft should have the right to package their products with automatic patching turned-on, so that patches are downloaded and installed automatically whether or not administrators want them. However, most administrators won’t agree to this, because they want to maintain control and don’t trust Microsoft. In that case, you should agree that the administrators who deploy and configure Windows systems should be considered responsible for keeping them patched properly.

Unfortunately, incidents like the Slammer worm, which propagated using unpatched Microsoft SQL 2000 servers, clearly indicate that not all administrators act responsibly when it comes to keeping their systems up-to-date with patches. To be fair, though, poorly patched systems are not always the fault of administrators: sometimes a third party vendor is not updating their applications, which prevent certain important patches, such as IE 9, to be installed. The point is that if Microsoft can’t control the patching process, then it’s pushed back onto the users and administrators and it must still be controlled and maintained.

Another thing to really consider is Practice. Once you’ve developed your patch management policy, you should periodically have your staff practice the procedures so the procedures become second nature.

Effective patch management has become a necessity in today’s information technology environments. Reasons for this necessity are:

1. The ongoing discovery of vulnerabilities in existing operating systems and applications
2. The continuing threat of hackers developing applications that exploit those vulnerabilities
3. Vendor requirements to patch vulnerabilities via the release of patches

These points illustrate the need to constantly apply patches to the computing environment. Such a large task is best accomplished following a series of repeatable, automated best practices. Therefore, it’s important to look at patch management as a closed-loop process. It is a series of best practices that have to be repeated regularly on your clients’ networks to ensure protection from exposed vulnerabilities. Patch management requires the regular rediscovery of systems that may potentially be affected, scanning of those systems for vulnerabilities, downloading patches and patch definition databases, and deploying patches to systems that need them.

Patching Resources

Microsoft updates arrive predictably on Patch Tuesday (the second Tuesday of every month), which means you can plan ahead for testing and deployment. You can get advance notice by subscribing to the security bulletin, which comes out three business days before with details of the updates.
Below is a list of currently available resources to use when augmenting your patch process, as well as some that can keep you informed of patch related updates that fall outside the scope of Microsoft updates.

- Patch Management.org (Patch Mailing List) - http://www.patchmanagement.org/
- Patch My PC (third party free patching) - http://www.patchmypc.net/

Best Practices in Patching with ConnectWise Automate

Utilize your Windows Patch Approval Policy across your managed and non-managed agents to report, push and for managed workstations automatically install Windows Updates.

Here are some critical items to consider around approving and deploying patches with ConnectWise Automate.

- A base set of patches can be approved that applies to 90-95% of client systems.
- You should be able to vary your patch approvals based on server or workstations.
- There will always be Exceptions. Those exceptions can be handled in specific patch deny or install groups.
- Approving patches on individual agents is not scalable.

ConnectWise Automate Ignite Specific Patch Settings

- All patch scheduling is completed at the Location Level within ConnectWise Automate and can be found under the Ignite Tab > Patching

Patching Screen Shot

- Agent must be in a ‘Patching Covered Under Contract’ group for a patch install window to be deployed
- Two Agent Exclusions from the Patch Install Window
  - Disable Automated Patch Install disables the application of a patch install template. ConnectWise Automate will not apply updates via a patch install window.
  - Disable All Patch Approval removes agents from the Windows Updates. Approved servers and workstations sub groups.
All Agents Should Have Your Patch Approval Policy

- TSP contract clients receive automated patching
- Non-TSP contract clients show all of the missing patches, but do not automatically receive patches
  - Use ConnectWise Automate Patch Reports to show missing patches
  - Discuss non-TSP contract clients’ patch status with them
  - Up sell your TSP service or charge labor for patching
  - Use ConnectWise Automate to implement your patch policy on their machines
- You should not patch all systems in a multi-site client on the same day and time
  - If a single bad patch takes out all of their offices at the same time, it is a bad day for everyone involved
- Monday – Sunday and Everyday are not enough options
  - We need patch install windows for a certain day of the week, day of the month, week of the month and the last day of the month
- Different types of servers need to be patched and rebooted at different times
  - Exchange servers need to see Active Directory during their reboot
  - Hyper-V hosts should be patched at a different time than their guest virtual machines
Evaluate and Approve your Patch Policy

- Your clients are paying you to manage their patching
- While the Automated Approval script will handle many patches based on categories, it will not make decisions on all patches available from Microsoft
- TSPs that do patch approval by hand and evaluate all patches will do a better job for their clients
- Designate a person responsible for patch approval
- Patches are evaluated and approved for later install during the scheduled patch install windows or pushed manually using ConnectWise Automate to install the approved patches on the computer
- Until you approve a hotfix for install, it will not be applied to agents by ConnectWise Automate
- Patch Tuesday drives your approval process
- Microsoft Patch Tuesday is the 2nd Tuesday of the month
  - There are occasional out of sequence releases
  - Wait and watch for the bleeding in mailing list and industry news
  - After a reasonable period, approve patches in ConnectWise Automate or approve following internal testing
  - Do not wait too long or feel the effects of Exploit Wednesday
- General approval guidelines
  - Drivers and language pack are generally ignored
  - Security patches and critical updates should default to install unless there is industry discussion of problems; security patches for items that you do not push to your customers, such as new IE or .Net versions, should still be approved
  - All default patch approval is done on the Windows Updates.Approved group
- Office updates and security patches should be approved on workstation and servers
  - Client applications may require Office components on servers
  - Citrix or terminal servers may run Office
  - Best practice is to approve them even if you do not have the requirement today
  - Security patches and updates will only install when there is a base application to install against
- Positive or neutral patch approval statuses
  - Not-Set: Patches set to Not-Set have not been classified yet; the goal should be that there
are no Not-Set patches on the Windows Updates. Approved group after patch approval each month

» Ignore: Passes on the patch, passively not approving it, but removing it from Not-Set status

» Install: Means the patch should be installed when the patch install command is sent to the agent either by patch install window or manual command

• Negative patch approval statuses

» Deny: Status overrides any other Not-Set, Ignore or Install patch approval setting anywhere in the system; Deny should only be used on specific exception groups and hardly ever on your base approval groups

» Remove: Remove status will not only stop a patch from being installed like Deny, but it also removes it from systems where it has already been installed. This is a bad practice. If the patch was not in your approval group but is working, removing it automatically could have serious effects on production systems. This should only be used in extreme cases.

• ConnectWise Automate Ignite automated approval

» There is a scheduled client script ‘Auto Approve Patches on Approved Group’ that will approve patches by categories, defined in the system properties.

» By default nothing is enabled; the properties must be switched from 0 to 1 to enable different categories

» Categories handled:

  • Approve critical updates - _sysPatchApproveCritical
  • Approve definitions - _sysPatchApproveDefinitions
  • Approve malicious removal tool - _sysPatchApproveMaliciousRemovalTool
  • Approve Microsoft Office - _sysPatchApproveOffice
  • Approve security updates - _sysPatchApproveSecurity
  • Approve service packs - _sysPatchApproveServicePacks
  • Ignore drivers - _sysPatchIgnoreDrivers
  • Ignore language packs - _sysPatchIgnoreLanguage

• Patch deny groups

» Patch deny statuses on the deny groups must be maintained for new patches issued by Microsoft in patch manager or on the groups Patches tab

» There is no process in place to automatically set the deny statuses on the deny groups
An agent in any group with a deny will override Not-Set, Ignore or Install statuses in other groups.

Groups are no longer drag and drop; membership is set on Agent > Info > Patching tab.

Scripts are available in Scripts > Maintenance > Patching that can be run against clients, locations, groups or search results to set the agent deny extra data fields.

- Service pack delivery
  - Service pack installs have a larger impact on your client than normal Microsoft updates in multiple ways and you must solve for these concerns.
  - Service packs are larger downloads; if you are deploying service packs, you should consider enabling ConnectWise Automate caching for sites with limited bandwidth or a high number of agents. For example, the offline installer for Windows 7 x64 is 903MB and when downloaded for multiple agents, you could crush the client’s Internet or WAN connectivity.
  - Service packs are rolling up large numbers of patches and are often adding new features; these changes require that you perform more diligence in evaluating service packs before approving them.
  - Available disk space is something you always need to consider when deploying service packs. For example, the offline installer for Windows 7 x64 Service Pack 1 requires 7.4Gb of free space on your system drive. The Patch Overrides built into ConnectWise Automate Ignite do verify this requirement, but it will result in service pack install failures if there is not enough disk space.
  - The install process for service packs is decidedly longer than normal patches. Install times can run 30 to 60 minutes with installs being spread out before and after a required reboot. Installing a service pack during work hours will dramatically impact employee productivity for your clients.

- Handling offline agents that miss their patch install windows
  - Best practice is to educate clients that their systems must be online and available during your documented maintenance window.
  - If workstations are continually offline during the maintenance window, there are methods to patch during work hours when the computer is available, but any maintenance performed during work hours potentially impacts employee productivity, which is counter to your goal of making them more efficient.
  - Ultimately, the patches you are deploying go to providing a stable and secure IT environment for the client and this should be your overriding concern.
  - ConnectWise Automate Ignite introduced the option to apply patch install windows during normal work hours for workstations that have repeatedly missed patch install windows.
• Set in the Location > Patching options, Day Time Patching is an option you must opt-in for on the location, before daytime patching will be applied.

• If you chose to use this option, you should proactively communicate why you are doing this with your client, how they can avoid it by allowing their agents to remain online during the support window and what impact they may experience.

• Consider the impacts of installing Windows updates while users are at work on those systems. Items to consider include bandwidth usage from patch downloads, CPU utilization as patches are being installed, reboot requests after patch installs and system performance if the pending reboot has not been allowed. Service pack installation magnifies each of these concerns.

• At the Location you can define the number of times a patch install window can be missed before the agent is placed into the daytime patch install window.

• Individual agents can be excluded from the location policy on the Agents > Info > Patching tab, so you can exclude the VP of Sales from the location policy.

• Systems with the Daytime Patch Install Window will have their patch reboot windows suppressed; instead the user will be prompted to handle the pending reboot. The prompt to reboot will default to No if the user does not answer, so that they must always opt-in for the reboot.

Cluster Patching

• Clusters are detected as part of role detection.

• Agents detected as cluster members are excluded from normal patching windows.

  » The regular ConnectWise Automate patch install process will break cluster installs, as the cluster members are not systematically handled computer by computer.

• You must use Client > Automate Ignite > Patching Cluster options or manually patch cluster members with ConnectWise Automate patching managing the cluster patching process.
Cluster patching requires another machine in the same location as the cluster that will act as a proxy in the process. Since current Windows clusters have a dependency on Active Directory, a domain controller at a minimum should always be available to fulfill this role. The process that is used in cluster patching is pretty simple in reality and is driven by this proxy and a PowerShell process that controls everything as follows:

1. Patching begins by locating the proxy and accessing the current state of the cluster
   a. Resource groups are analyzed and recorded
   b. Node states are recorded as well
2. A node is evacuated and all service groups and resources are passed to a different node
3. The first node is then patched and rebooted
4. The proxy watches the reboot process and once complete, repopulates the freshly patched node
5. The next node is then evacuated and patched and then rebooted
6. This continues until all nodes are complete
7. The proxy then resets the cluster configuration back to the original state as recorded by the initial assessment
The entire patching process is controlled and monitored by the proxy machine and at any point if a node fails to come back online, the process is halted so as not to put the cluster in an unstable state and every step is logged (see below) to ensure the TSP can determine what went wrong and what node is impacted.

Cluster Patching Process Log

At implementation time, ConnectWise Automate Software was the only RMM vendor offering a process similar to this and it was designed to automate the once fully manual process of patching clusters so that TSPs could sleep easier and do a better job of keeping clusters up to date for their clients.
Appendix A: Sample Service Agreement

Sample Only – All Legal Documents Should Be Reviewed By A Qualified Attorney

Replace <Your Company> with your company’s name and <CLIENT> with your client’s name.

Sample Service Agreement

<Client Name>

(Address 1)

(Address 2)

(City, State, Zip)

<Date of Agreement>

This Service Agreement (“Agreement”) is made this______day of_______, 20______ by and between <CLIENT Name> (CLIENT/Account) located at <CLIENT Address> and <Your Company>, located at <Your Company Address>.

WHEREAS, <Your Company> is a provider of Managed Network Services;

WHEREAS, CLIENT desires to contract with <Your Company> for the provision of the <Your Company> Monitoring Services Solutions;

NOW THEREFORE, for and in consideration of the premises contained herein and good and valuable consideration, receipt of which is hereby acknowledged, the parties agree as follows:

Service Period

This Agreement shall be effective as of the date of this Agreement, executed by CLIENT unless sooner terminated in accordance with the terms hereof, and shall be for an initial term of twelve (12) months. CLIENT and <Your Company> reserve the right to review this agreement quarterly.

Continuance / Automatic Renewal

This Agreement shall renew automatically at the end of the prior Agreement term for a period of twelve (12) months unless <Your Company> or the CLIENT affirmatively terminates it in accordance with the conditions set forth in this Agreement.
### Purchase Price

CLIENT is purchasing <Your Company> Program Services under this Agreement for the purchase price outlined in Appendix A.4. Said purchase price shall be paid in monthly installments with the first installment due upon execution of this agreement. Each payment thereafter shall be due the first day of each calendar month. Services provided hereunder shall be assessed against this Account as provided herein.

### Charges for Service Delivery

Services shall be charged against the Account in accordance with the terms and conditions as outlined in Appendix A.4, and the Rate Card in Appendix A.3.

Any supplemental services provided by <Your Company> which are outside the terms of this Agreement, including but not limited to, any maintenance provided beyond normal business hours and services in excess of the Account purchased herein, shall be charged to CLIENT as an additional charge in accordance with the terms and conditions as outlined in Appendix A.1. Any additional billing charges will be invoiced at the end of each month, with payment expected within thirty (30) days, unless otherwise specified by <Your Company>.

CLIENT shall, in addition to the other amounts payable under this Agreement, pay all sales and other taxes, federal, state, or otherwise, however designated, which are levied or imposed by reason of the services provided pursuant to this Agreement. Without limiting the foregoing, CLIENT shall promptly pay to <Your Company> an amount equal to any such taxes actually paid or required to be collected or paid by <Your Company>.

<Your Company> reserves the right to refuse or suspend service under this Agreement in the event CLIENT has failed to pay any invoice within thirty (30) days of said invoice date, whether it be an invoice for services provided under this Agreement or any other agreement between the parties.

### Devices Covered

<Your Company> reserves the right to renegotiate rates based on additions of locations, hardware, software, hardware support requirements, and/or services as well as modify this Agreement (or any portion thereof) with a 30-day notice.

For purposes of this Agreement, the Network shall include all locations as outlined in Appendix A.1. In addition, this agreement is based on services provided to those devices listed in Appendix A.2. Any additional devices added to the network without the consent or acknowledgment of <Your Company> will not be honored or supported by <Your Company> under this agreement. Please review this agreement from time to time so that you will be apprised of any changes.

### Conditions of Service

The CLIENT Network is eligible for monitoring and support under this Agreement provided it is in good condition and <Your Company> serviceability requirements/standards and site environmental conditions are met. <Your Company> reserves the right to inspect the Network upon the commencement of the term of this agreement for the purpose of creating a diagram of the Network and/or conducting a diagnostic test of the...
Network. Unless stated otherwise, said inspection shall be charged against the Account using our standard hourly billing rates.

<Your Company> shall not be responsible to CLIENT for loss of use of the Network or for any other liabilities arising from alterations, additions, adjustments or repairs which have been made to the Network other than by authorized representatives of <Your Company>.

<Your Company> reserves the right to suspend or terminate this Agreement if in its sole discretion, conditions at the service site pose a health or safety threat to any <Your Company> representative.

Service Responsibility of <YOUR COMPANY>

<Your Company> will provide remote and/or on-site services under the following conditions using the following bill rates, unless otherwise specified in Appendix A.3.

<table>
<thead>
<tr>
<th>Time of Service</th>
<th>Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Hours</td>
<td></td>
</tr>
<tr>
<td>Monday – Friday, 8:00am – 5:00pm</td>
<td>Onsite: $135 / hour</td>
</tr>
<tr>
<td></td>
<td>Remote: $95 / hour</td>
</tr>
<tr>
<td>After Hours</td>
<td></td>
</tr>
<tr>
<td>Monday – Friday, 5:00pm – 11:00pm</td>
<td>Onsite: $180 / hour</td>
</tr>
<tr>
<td>Saturday, 9:00am – 5:00pm</td>
<td>Remote: $135 / hour</td>
</tr>
<tr>
<td>Overnight</td>
<td></td>
</tr>
<tr>
<td>Monday – Friday, 11:00pm – 8:00am</td>
<td>Onsite: $240 / hour</td>
</tr>
<tr>
<td>Saturday 5:00pm – Monday 8:00am</td>
<td>Remote: $190 / hour</td>
</tr>
<tr>
<td>Holidays</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Onsite: $275 / hour</td>
</tr>
<tr>
<td></td>
<td>Remote: $250 / hour</td>
</tr>
</tbody>
</table>

Holidays Observed and Service Support Hours

<table>
<thead>
<tr>
<th>Holiday</th>
<th>Date</th>
<th>Service Support Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Year’s Day</td>
<td>January 1st</td>
<td>N/A</td>
</tr>
<tr>
<td>Memorial Day</td>
<td>Last Monday in May</td>
<td>10:00am – 3:00pm</td>
</tr>
<tr>
<td>Independence Day</td>
<td>July 4th</td>
<td>N/A</td>
</tr>
<tr>
<td>Labor Day</td>
<td>1st Monday in September</td>
<td>N/A</td>
</tr>
<tr>
<td>Thanksgiving Day</td>
<td>4th Thursday in November</td>
<td>N/A</td>
</tr>
<tr>
<td>Christmas Day</td>
<td>December 25th</td>
<td>N/A</td>
</tr>
</tbody>
</table>

It is the responsibility of the CLIENT to promptly notify <Your Company> of any events/incidents that could impact the services defined within this agreement and/or any supplemental service needs, and for <Your Company> to respond in a timely manner via phone, email, remote access, and/or on-site services as defined in Appendix A.3 of this Agreement.

a) If services are requested by the CLIENT outside of normal business hours, <Your Company> shall provide such service subject to the availability of its representatives, according to the terms and conditions set forth in this Agreement.
b) <Your Company> shall monitor, advise, and provide supplemental services as defined in this agreement during business hours, unless otherwise specified in Appendix A.3, and in accordance with <Your Company>'s Network policies then in effect. <Your Company> shall provide scheduled remote and onsite support services in accordance with this agreement. <Your Company>'s representatives shall have and the CLIENT shall provide full access to the Network in order to affect the necessary monitoring and/or supplemental services. All services defined in this Agreement shall be provided during regular business hours, unless otherwise specified in Appendix A.3.

c) <Your Company> shall be obligated to provide service only at the Service Site(s) defined in this agreement as outlined in Appendix A.1. If the CLIENT desires to relocate, add or remove locations, the CLIENT shall give appropriate notice to <Your Company> of its intention to relocate sixty (60) days in advance. <Your Company> reserves the right to renegotiate service terms with respect to any relocation and/or addition of locations by the CLIENT. Such right includes the right to refuse service to Network at the relocation and/or new site.

d) <Your Company> is obligated to provide CLIENT with Service Agreements higher-priority response for emergency as well as non-emergency service requests.

How to Contact Service Desk

Telephone: (877) 123-4567
Web: www.yourcompany.com/support
Email: support@yourcompany.com

Preferred Contact Method: Create Tickets from the Remote Tray

The Remote Tray is an executable that runs on the remote agent computer and allows customers to interact with the technicians. Customers can send in their inventory status, screenshots and create service tickets.

The tray is accessed by clicking on the taskbar icon on the remote agent computer. To create a new ticket from a remote agent:

On the desktop of an agent machine, right-click the TSP logo in the taskbar and select Create Service Ticket.

a) Enter the requestor's email address into the From field. Any additional email addresses that should be emailed with ticket information can be entered into the CC field. Each additional email address must be separated by a semi-colon (;).

b) Enter the ticket Subject and a detailed description just below the Subject.
c) Select the ticket priority from the Importance drop-down. Available options are: Low, Normal, High and Emergency. All tickets will default to ‘Normal’.

d) Click the Attach Screenshot button to attach a screenshot of your desktop. To remove the screenshot from the ticket, click Remove Screenshot.

e) Click Send to send the ticket

**Things to Do Before Contacting Support**

When you call or send a message, please ensure that you have the following detailed and complete information:

- Your name and location and where and how to contact you in case of a problem
- A description of the problem and its severity
- Any error messages and what was processing at the time the problem occurred
- The applications and versions you’re working with
- Any changes made recently
- In case of a request or question, a description of request or question and relevant details

**Client Responsibilities**

1. CLIENT shall provide adequate workspace, heat, light, ventilation, electric current and outlets, internet, remote access, and long-distance telephone access for use by <Your Company>’s representatives.

2. CLIENT agrees that it will inform <Your Company> of any modification, installation, or service performed on the Network by individuals not employed by <Your Company> in order to assist <Your Company> in providing an efficient and effective Network support response time.

3. CLIENT will designate a managerial level representative to authorize all Network Support Services. Whenever possible, said representative shall be present whenever a <Your Company> service representative is on-site. This contact information shall be outlined in Appendix A.1, and it is the CLIENT’s responsibility to inform <Your Company> of any changes made to this representation thirty (30) days in advance.

4. CLIENT agrees that a maintenance window must be established and honored to allow for proper system maintenance, patching and reboots.

**Scope of Technology Solution Agreement**

This Agreement is designed to provide the Account with centralized, proactive monitoring supplemental services for certain Networking System. This Agreement includes:

LOCATION(S): Specific location(s) to be covered by this agreement can be found in Appendix A.1.
Service Limitations

In addition to other limitations and conditions set forth in this Agreement, the following service and support limitations are expressed:

a. Cost of consumables, replacement parts, hardware, software, network upgrades and associated services are outside the scope of this agreement. <Your Company> will provide consultative specification, sourcing guidance and/or Time and Material/Project offerings.

b. Except as otherwise stated in Appendix A.2 of this agreement all Server, Network Device and Software upgrades are outside the scope of this agreement.

c. Manufacturer warranty parts and labor/services are outside the scope of this agreement.

d. Periodic reboots for such devices as firewalls, routers, and servers are required to apply/activate critical update patches and configuration changes. <Your Company>’s support services within this agreement are predicated upon the CLIENT’S support and commitment to providing time/scheduling for network device reboots with its staff and/or users support.

e. Application software support is limited to the manufacturer’s products listed in Appendix A.2: Printer maintenance support is limited to non-warranty servicing of printer products listed in Appendix A.2.

f. Virus mitigation within the scope of this agreement is predicated on CLIENT satisfying recommended backup schemes and having appropriate Antivirus Software with current updates.

g. Restoration of lost data caused by systems/hardware failure is outside the scope of this agreement.

h. This agreement and support services herein are contingent on CLIENT’S permission of <Your Company> having secure remote access into CLIENT’S network (eg. VPN, Citrix/Terminal Server, Telnet, SSH, RAS or other solution expressly approved by <Your Company>). Depending on the remote access solution used, additional charges may apply to the contract.

i. Support services required or requested outside the scope of this agreement may not be exchanged for days or services within this agreement. Outside of scope support services are available and will be provided on either a Time and Material, or Project basis.

Warranties and Disclaimers

<Your Company> makes and the CLIENT receives no warranty, express or implied, and all warranties of merchantability and fitness for a particular purpose are expressly excluded. In no event shall <Your Company> or any of its Directors, Employees or Other Representatives be responsible for any special, incidental, indirect, or consequential damages of any kind including, without limitations, those resulting from loss of data, income, profit, and on any theory of liability, arising out of or in connection with the services or use thereof even if it has been advised or has knowledge of the possibility of such damages. The CLIENT shall assume full responsibility for the overall effectiveness and efficiency of the operating environment in which the Network is to function.

Indemnification

CLIENT hereby agrees to indemnify and defend at its sole expense: <Your Company>, its employees, agents, representatives, directors and shareholders, from and against any and all claims arising out of or based upon CLIENT’S use of all services, software or hardware provided or serviced hereunder, including, but not limited to, claims based on software licensing violations, copyright infringement, trademark infringement and patent infringement. In addition, CLIENT agrees to pay any judgment and costs associated with such claim.
Opt-Out/Termination

<Your Company> and/or CLIENT shall have the right to terminate this Agreement under any of the following conditions:

- If one of the parties shall be declared insolvent or bankrupt.
- If a petition is filed in any court and not dismissed in ninety days to declare one of the parties bankrupt and/or for a reorganization under the Bankruptcy Law or any similar statute.
- If a Trustee in Bankruptcy or a Receiver or similar entity is appointed for one of the parties.
- If the CLIENT does not pay <Your Company> within thirty (30) days from receipt of <Your Company>’s invoice and/or otherwise materially breaches this Agreement.
- If <Your Company> fails to perform its obligations under this Agreement and such failure continues for a period of thirty days after written notice of the default, the CLIENT shall have the right to terminate this Agreement.
- Either party may terminate this Agreement upon sixty days (60) written notice.

Upon termination, all hardware and software installed by <Your Company> that was required to conduct network support services are the property of <Your Company> and will be surrendered and returned to <Your Company> at end of the agreement.

Non-Hire/Non-Disclosure

Because employees are one of our most valuable assets, policy and professional ethics require that our employees not seek employment with, or be offered employment by any CLIENT during the course of engagement and for period of one (1) year thereafter. Your signature on this document confirms your organization’s agreement to adhere to this professional standard of conduct.

CLIENT acknowledges that <Your Company> is involved in a highly strategic and competitive business. CLIENT further acknowledges that CLIENT would gain substantial benefit and that <Your Company> would be deprived of such benefit, if CLIENT were to directly hire any personnel employed by <Your Company>. Except as otherwise provided by law, CLIENT shall not, without the prior written consent of <Your Company>, solicit the employment of <Your Company> personnel during the term of this Agreement and for a period of one (1) year following expiration of this Agreement.

CLIENT agrees that <Your Company> damages resulting from breach by CLIENT of this provision would be impracticable and that it would be extremely difficult to ascertain the actual amount of damages. Therefore, in the event CLIENT violates this provision, CLIENT shall immediately pay <Your Company>an amount equal to 60% of employee’s total annual compensation, as liquidated damages and <Your Company> shall have the option to terminate this Agreement without further notice or liability to CLIENT. The amount of the liquidated damages reflected herein is not intended as a penalty and is reasonably calculated based upon the projected costs <Your Company> would incur to identify, recruit, hire and train suitable replacements for such personnel.

This Confidentiality, Privacy and Compliance portion of this Agreement is in addition to other terms and conditions set forth in any and all contracts currently existing or hereafter created between CLIENT and <Your Company>. This agreement shall under no circumstances be deemed to alter any such contract except as specifically provided below.
<Your Company> acknowledges that in the course of providing services to said CLIENT, <Your Company> may learn from CLIENT certain non-public personal and otherwise confidential information relating to said CLIENT, including its customers, consumers or employees. <Your Company> shall regard any and all information it receives which in any way relates or pertains to said CLIENT, including its customers, consumers or employees as confidential.

<Your Company> shall take commercially reasonable steps to not disclose, reveal, copy, sell, transfer, assign, or distribute any part or parts of such information in any form, to any person or entity, or permit any of its employees, agents, or representatives to do so for any purpose other than purposes which serve CLIENT or as expressly and specifically permitted in writing by said CLIENT or as required by applicable law.

Said CLIENT acknowledges that it also has responsibility to keep records and information of its business, customers, consumers, and employees, confidential.

Said CLIENT also acknowledges that all information and services, consulting techniques, proposals, and documents disclosed by <Your Company> or which comes to its attention during the course of business and provided under this agreement constitute valuable assets of, and confidential and/or proprietary to <Your Company>.

This provision shall survive termination of this Agreement and any other agreements between CLIENT & <Your Company>.

Insurance

<Your Company> shall maintain at its sole expense commercial general liability insurance for personal injury and property damage for a general aggregate of $2,000,000; Professional Liability insurance (AKA Errors & Omissions Liability insurance) for a general aggregate of $1,000,000; worker’s compensation insurance as required by law; and hired and non-owned automobile liability insurance for the combined single limit of $1,000,000. At CLIENT’s request, <Your Company> further agrees to furnish CLIENT with certificates, including renewal certificates, evidencing such coverage within thirty (30) days of commencing performance under this Agreement, at every renewal and at other times as may be reasonably requested by CLIENT.

General Provisions

a. Sole Agreement: This Agreement constitutes the entire and only understanding and agreement between the parties hereto with respect to the subject matter hereof and, except as expressly set forth herein, may be amended only by a writing signed by each of the parties hereto.

b. Severability: If a court of competent jurisdiction determines that any terms or provision of this Agreement are invalid or unenforceable; such determination shall not affect the validity or enforceability of the remaining terms and provisions of this Agreement, which shall continue to be given full force and effect.

c. Captions: The captions of the paragraphs of this Agreement are for convenience only and shall not affect in any way the meaning or interpretation of this Agreement or any of the provisions hereof.

d. Binding Effect: This Agreement shall be binding upon, and shall inure to the benefit of, the parties hereto and their heirs, legal representatives, personal representatives, administrators, successors, and permitted assigns, as the case may be.
e. Waiver: Any failure of either party to comply with any obligation, covenant, agreement, or condition herein may be expressly waived, but only if such waiver is in writing and signed by the other parties. Any such waiver or failure to insist upon strict compliance with such obligation, covenant, agreement, or conditions shall not operate as a waiver of and/or set precedence with respect to any subsequent and/or other failure.

f. Governing Law: Notwithstanding the place where this Agreement may be executed by any party, this Agreement, the rights and obligations of the parties, and any claims and disputes relating hereto shall be subject to and governed by the laws of the State of <YOUR STATE> as applied to agreements among <YOUR STATE> residents to be entered into and performed entirely within the State of <YOUR STATE>, and such laws shall govern all aspects of this Agreement. The parties agree to submit to the personal jurisdiction and venue of the state and federal courts in the State of <YOUR STATE>, in the Judicial Circuit where <Your Company> has its principal office, for resolution of all disputes and causes of action arising out of this Agreement, and the parties hereby waive all questions of personal jurisdiction and venue of such courts, including, without limitation, the claim or defense therein that such courts constitute an inconvenient forum.

g. Assignment: This Agreement and the rights and duties hereunder shall not be assignable by either party hereto except upon written consent of the other.

h. Force Majeure: <Your Company> shall not be liable for any problems due to external causes beyond its control including, but not limited to, terrorist acts, natural catastrophe, fire, flood, or other act of God, and/or power failure, virus propagation, improper shut down of the Network and related Network Systems/Services.

i. Attorneys’ Fees. In any action between the parties to enforce any of the terms of this Agreement, the prevailing party shall be entitled to recover all expenses, including reasonable attorneys’ fees.

j. IN WITNESS WHEREOF, the parties have executed this Agreement as of the day and year first below written.

**Remedies**

In the event CLIENT terminates this Agreement for any reason other than a breach of the terms herein, CLIENT shall be entitled to a refund of any monies extended in advance of the month or part thereof for which services by <Your Company> were last performed.

**Acceptance**

<table>
<thead>
<tr>
<th>&lt;Your Company&gt;</th>
<th>&lt;CLIENT&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td>Signature:</td>
</tr>
<tr>
<td>Printed Name:</td>
<td>Printed Name:</td>
</tr>
<tr>
<td>Title:</td>
<td>Title:</td>
</tr>
<tr>
<td>Date:</td>
<td>Date:</td>
</tr>
</tbody>
</table>
Technology Solution Offering

Description

<Your Company> offers a comprehensive and fully configurable (up to 24x7) service offering that provides reactive and proactive support for your IT applications for both Commercial Off-The-Shelf (COTS) configurations and custom (in-house) applications. By applying regular monthly maintenance tasks to the network backbone we will be able to reduce the likelihood and frequency of network failures and issues, thus saving the customer money (and time) in unforeseen downtime. The monitoring solution we put in place also assures we have all the information we need to make meaningful suggestions and also helps to ensure we know of issues as early as the customer. In this we will be in a position that allows us to service and solve unforeseen issues with great speed, so that each issue takes less time to resolve. By combining these two activities, we can reduce the overall cost of our customer’s network while at the same time creating a more stable and optimized network environment. This will be backed up regularly with scheduled Health reviews with the customer in which we will be reviewing reports with the customer and therefore providing them with a level of transparency they have not been able to achieve to this point.

Benefits

Reduced overheads. Managed IT services are a cost effective method for managing your business’ IT requirements as you do not need to hire IT staff in house. Having an IT department in house can be costly especially if you do not require the services of IT experts on a daily basis. By outsourcing your IT department you are able to only pay for IT support when you need it and as you need it.

Increased efficiency. Outsourcing IT support also allow you to increase business productivity and efficiency as you are able to focus on what you do best, rather than having to solve complex IT problems.

Scalability. You have a team of IT experts – not just one – on hand, at your demand to help solve IT problems as they arise, no matter how big or small.

Customized Plans. You can customize your managed IT services plan to suit your business needs and budgets. Pay per device, pay as you go, pay by the number of IT support hours required each month or the level of monitoring and maintenance required – you decide.

Accountability. Your IT services provider is accountable for the functionality and performance of their services. Running complex IT infrastructure can be quite expensive and involving. Technology solutions give you the assurance that someone else is accountable for the delivery of the services that you require. It also means that you can direct your resources to your core business.
## Services Included

Our Technology Solution program is designed to provide:

<table>
<thead>
<tr>
<th>Core Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Monitoring</td>
<td>Monitoring the customer’s servers for any issues that may arise.</td>
</tr>
<tr>
<td>Backup Monitoring</td>
<td>Monitoring the success of the customer’s backup solution to ensure that their data is always protected.</td>
</tr>
<tr>
<td>Network Monitoring</td>
<td>Monitoring the customer's routers and switches to ensure that network traffic is always moving.</td>
</tr>
<tr>
<td>Workstation Monitoring</td>
<td>Monitoring the customer's workstations for any issues that may arise to ensure optimum performance.</td>
</tr>
<tr>
<td>Automated Maintenance</td>
<td>Basic automated maintenance and self-healing solutions applied to customers’ servers, workstations.</td>
</tr>
<tr>
<td>Patch Management</td>
<td>Monitoring and management of patch levels; ensuring desktops, servers are kept up to date.</td>
</tr>
<tr>
<td>Application Monitoring</td>
<td>Monitoring customers' email availability, Outlook web access, SQL Database, and Terminal Services.</td>
</tr>
<tr>
<td>Endpoint Security (ESM)</td>
<td>Apply a complete security management system to customers’ environment, including: antivirus, antispyware, and anti-malware management.</td>
</tr>
<tr>
<td>Performance Reporting</td>
<td>Monthly / quarterly CIO meetings to review customized reports, overall network health, and strategic IT planning with customer.</td>
</tr>
</tbody>
</table>
Appendix A.1 – Contact Information

Account Representative

Your <Your Company> Account Representative / Primary Contact is <INSERT NAME HERE>. Please contact <him/her> if you wish to make any changes to, or ask questions about your service agreement with us.

You can contact your account representative in the following ways:

- Telephone: (555) 555-5555
- Mobile: (555) 555-1234
- Email: sales@yourcompany.com

Client Information

The primary CLIENT contact is: <INSERT NAME HERE>

>Title>

Location:

Phone:

Fax:

Email:

The secondary CLIENT contact is: <INSERT NAME HERE>

>Title>

Location:

Phone:

Fax:

Email:

Changes to this agreement may only be requested by the persons named above. It is the responsibility of the CLIENT to notify <Your Company> of changes to the contact person.
This agreement covers the following CLIENT locations:

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Address</th>
<th>Phone</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Office</td>
<td>123 Any St., Anytown, ST 12345</td>
<td>(800) 555-1212</td>
<td>Roger Contact</td>
</tr>
</tbody>
</table>

This agreement allows for the following CLIENT Maintenance Windows:

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Task</th>
<th>Day</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Office</td>
<td>Workstation Patching</td>
<td>Everyday</td>
<td>3 AM – 5 AM</td>
</tr>
<tr>
<td>Main Office</td>
<td>Server Patching</td>
<td>Sunday</td>
<td>3 AM – 5 AM</td>
</tr>
<tr>
<td>Main Office</td>
<td>Workstation Reboots</td>
<td>Everyday</td>
<td>3 AM – 6 AM</td>
</tr>
<tr>
<td>Main Office</td>
<td>Server Reboots</td>
<td>Sunday</td>
<td>3 AM – 6 AM</td>
</tr>
<tr>
<td>Main Office</td>
<td>Routine Maintenance Items</td>
<td>Everyday</td>
<td>12 AM – 3 AM</td>
</tr>
</tbody>
</table>
Appendix A.2 –
Device Identification and Preventative Checklist

This agreement is based on the following information agreed upon by you. Any changes to this information require an updated service agreement.

DEVICES SUPPORTED BY THIS AGREEMENT

The following devices are covered by this agreement:

<table>
<thead>
<tr>
<th>Device</th>
<th>Type</th>
<th>Serial #</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASA 5510 Firewall</td>
<td>Network</td>
<td>LJ890-756-983</td>
<td>Main Office</td>
</tr>
<tr>
<td>Exchange/Mail Server</td>
<td>Server</td>
<td>DW67IF</td>
<td>Main Office</td>
</tr>
<tr>
<td>Domain Controller Network</td>
<td>Server</td>
<td>W148D7</td>
<td>Main Office</td>
</tr>
<tr>
<td>Fileserver</td>
<td>Server</td>
<td>5487-9865-854</td>
<td>Main Office</td>
</tr>
<tr>
<td>Dell Switch</td>
<td>Network</td>
<td>S457DW</td>
<td>Main Office</td>
</tr>
</tbody>
</table>

Since part of this service agreement includes device support, CLIENT is responsible for informing <Your Company> of changes to the number of devices within five (5) business days.

Under this agreement, the CLIENT is entitled to a quantity (Actual Number (5)) of supported devices as defined in the Program Description. Any additional devices added to program will have an incremental cost of $XXX.00 per month per network device, $XXX.00 per month per server and, $XXX.00 per month per workstation device. The monthly pricing will be automatically updated with the addition of a device.

<Your Company> support and maintenance is limited to items, services, hardware and applications found on the following lists:

Applications: Windows 7, Windows 2008, MS Exchange 2010, MS SQL 2008, MS Outlook 2010, MS Office 2010, Applications, more...

Firewalls: Cisco ASA 5510<models>, more...

Other Devices: routers <models>, switches <models>, printers <models>, more...
Preventative Maintenance Checklist

<table>
<thead>
<tr>
<th>Description</th>
<th>Daily</th>
<th>Weekly</th>
<th>Monthly</th>
<th>Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventative Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real Time System Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virus Definition Updates</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real Time Virus Scanning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deep Virus Scanning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workstation Security Patches</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Security Patches</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Log Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temporary File Removal</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defragmentation of Workstation Hard Drives</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Error Checking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Space Checking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review and Planning Meeting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Appendix A.3 – Service Desk, Response Times and Rates

<Your Company> Service Desk Services

The <Your Company> Service Desk provides a point of escalation for your company when they have an issue or question. <Your Company>’s staff is available during business hours to log issues and support your team. You can contact the IT Service Desk via email or phone. We commit to responding to your question promptly (response times guaranteed, based on severity). If you are contacting us to escalate a service outage, we will route the call to our technical center for prompt attention.

Emergency Support Issues

Our Technology Solution Program enables access to emergency support services when the need arises. Should your team detect an issue with a service or device outside standard business hours, you can contact the Emergency Support team to report the issue. <Your Company>’s team (security or network, as appropriate) will investigate the issue and act appropriately.
Service Desk Severity and Response Times

<table>
<thead>
<tr>
<th>Problem Severity</th>
<th>Initial Response Time</th>
<th>Escalation</th>
<th>Expected Time to Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency (Business Hours)</td>
<td>1 hour</td>
<td>N/A</td>
<td>Determined by the nature of the event – normally 4 hours</td>
</tr>
<tr>
<td>Critical – Site Impact</td>
<td>2 hours/next business day</td>
<td>1 Hour</td>
<td>Determined by the nature of the event – normally 8 hours</td>
</tr>
<tr>
<td>Major – Departmental Impact</td>
<td>4 hours/next business day</td>
<td>4 Hour</td>
<td>Determined by the nature of the event – normally 8 hours</td>
</tr>
<tr>
<td>Normal – User Impact</td>
<td>8 hours/next business day</td>
<td>8 Hour</td>
<td>Determined by the nature of the event</td>
</tr>
<tr>
<td>Nuisance Issues</td>
<td>16 hours/2nd business day</td>
<td>4 Hour</td>
<td>Determined by the nature of the event</td>
</tr>
</tbody>
</table>

Service/Incident Escalations

As not every support case can be resolved at the point of report, it is important to outline the process by which cases are and can be escalated.

Functional Escalations

As outlined in the Service Desk Severity and Response Times chart above, our service desk team will escalate any unresolved issue(s) to our Operations team within the time allotted for that severity level.

Hierarchical Escalations

If you have questions or concerns about the operation of the service desk, wish to compliment the team, or simply require more information about an incident; please contact your account representative to gain more insight.

Rate Card (if not included in Service Offering)

<table>
<thead>
<tr>
<th>Time of Service</th>
<th>Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Hours</td>
<td></td>
</tr>
<tr>
<td>Monday – Friday, 8:00am – 5:00pm</td>
<td>Onsite: $135 / hour</td>
</tr>
<tr>
<td></td>
<td>Remote: $95 / hour</td>
</tr>
<tr>
<td>After Hours</td>
<td></td>
</tr>
<tr>
<td>Monday – Friday, 5:00pm – 11:00pm</td>
<td>Onsite: $180 / hour</td>
</tr>
<tr>
<td>Saturday, 9:00am – 5:00pm</td>
<td>Remote: $135 / hour</td>
</tr>
<tr>
<td>Overnight</td>
<td></td>
</tr>
<tr>
<td>Monday – Friday, 11:00pm – 8:00am</td>
<td>Onsite: $240 / hour</td>
</tr>
<tr>
<td>Saturday 5:00pm – Monday 8:00am</td>
<td>Remote: $190 / hour</td>
</tr>
<tr>
<td>Holidays</td>
<td></td>
</tr>
<tr>
<td>As listed in Holidays Observed and</td>
<td>Onsite: $275 / hour</td>
</tr>
<tr>
<td>Support Hours</td>
<td>Remote: $250 / hour</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix A.4 – Monthly Pricing Structure

The cost of the <Service Name> program is based upon several key factors:

1. Base program cost that includes monitoring of <##> devices. These are the devices that have been identified in Appendix A.2 that will require maintenance, monitoring and support as determined by your organization’s critical business functions (email, internet, file sharing etc).

2. Any additional servers or devices that exceed the device limit of the <Service Name> Program.

3. Inclusion of any optional modules over and above the base program.

4. Total number of monthly pre-scheduled maintenance hours or block of hours that are required to maintain said devices, as determined by <Your Company>

5. Any additional dispatch, support or emergency fees

6. Any special line of business applications or conditions that exist.

Monthly Maintenance Monitoring and Support

The <Service Name> service program includes pre-scheduled onsite and/or remote support and maintenance. Based on the number of users and devices within your organization, <Your Company> will commit to having a technician onsite or working remotely from our Network Operation Center on a scheduled basis to assist you with any IT related issues or questions.

Based on this information, the monthly program price for <CLIENT> has been determined to be: <$>, summarized in the table below:

<table>
<thead>
<tr>
<th>Program Components</th>
<th>Component Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Program Fee (which includes &lt;#&gt; devices:</td>
<td>$</td>
</tr>
<tr>
<td>Additional Servers / Devices</td>
<td>$</td>
</tr>
<tr>
<td>Initial Setup Fee</td>
<td>$</td>
</tr>
<tr>
<td>TOTAL PROGRAM COST</td>
<td>$</td>
</tr>
</tbody>
</table>
Appendix B: Client Standards Checklist

Client Name:                                                                      Location:

Desktop PCs and Notebooks/Laptops

• All Desktop PCs and Notebooks/Laptops with Microsoft Operating Systems running
• Windows Vista Pro or later
• All Desktop PCs and Notebooks/Laptops with Microsoft Operating Systems have all of the latest
  Microsoft Service packs and Critical Updates installed
• All Non-Microsoft PCs and Notebooks/Laptops must meet similar OS-Specific requirements such as the
  latest version of the OS as supplied
• All Desktop PC and Notebook/Laptop Software must be Genuine, Licensed and Vendor-Supported
• All Desktops PCs and Notebooks have a minimum of 2GB Ram and 80GB Hard Drives

Servers

• All Servers with Microsoft Operating Systems running Windows Server 2008 or later
• All Servers with Microsoft Operating Systems have all of the latest Microsoft Service Packs and Critical
  Updates installed
• All Server Software must be Genuine, Licensed and Vendor-Supported
• All Servers have at a minimum 25% free space on all drives that are currently installed and partitioned

Environmental Conditions (Unless Being Supplied As Part of Technology Solution Contract)

• The environment must have a currently licensed, up-to-date and Vendor-Supported Server- based
  Antivirus/Spyware Solution protecting all Servers, Desktops, Notebooks/Laptops, and Email
• The environment must have a currently licensed, up-to-date and Vendor-Supported Anti-Spam
  Solution
• The environment must have a currently licensed, Vendor-Supported Server or Network- based Backup
  Solution
• The environment must have a currently licensed, Vendor-Supported Firewall between the Internal
  Network and the Internet
• All Wireless data traffic in the environment must be securely encrypted- Traffic should be segmented
  for public vs. private
• The environment must have a T1 or other form of High-Speed Internet Access with Static IPs

Comments:
### Appendix C: Client Onboarding Information

**Client Name:**

---

#### Client Info

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Contact Person</td>
<td></td>
</tr>
<tr>
<td>Office Phone</td>
<td></td>
</tr>
<tr>
<td>Mobile Phone</td>
<td></td>
</tr>
<tr>
<td>Home Phone</td>
<td></td>
</tr>
<tr>
<td>E-mail Address</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Location Name</td>
<td></td>
</tr>
</tbody>
</table>

#### Domain Name Info

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td></td>
</tr>
<tr>
<td>Registrar Name</td>
<td></td>
</tr>
<tr>
<td>Domain Created</td>
<td></td>
</tr>
<tr>
<td>Domain Expires</td>
<td></td>
</tr>
<tr>
<td>DNS Servers</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>MX Record(s)</td>
<td></td>
</tr>
<tr>
<td>A Record(s)</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td>Misc. Information</td>
<td></td>
</tr>
</tbody>
</table>
## ISP Info

| ISP |  
| Internet type (DSL/T-1) |  
| Bandwidth |  
| Dynamic or Static |  
| Usable IP Range |  
| Subnet |  
| Gateway |  
| ISP Tech Support Phone Number |  
| ISP Tech Support E-mail |  
| User Account |  
| Password |  
| Misc. Information |  

## Web and E-mail Hosting

| Website Hosted On |  
| Email Hosted On |  
| User Account |  
| Password |  
| Misc. Information |  

<table>
<thead>
<tr>
<th>Server Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make &amp; Model</td>
</tr>
<tr>
<td>Purchase Date</td>
</tr>
<tr>
<td>Serial Number</td>
</tr>
<tr>
<td>Warranty Information</td>
</tr>
<tr>
<td>CPU</td>
</tr>
<tr>
<td>RAM</td>
</tr>
<tr>
<td>RAID Configuration</td>
</tr>
<tr>
<td>SCSI</td>
</tr>
<tr>
<td>Battery Backup</td>
</tr>
<tr>
<td>Server Name</td>
</tr>
<tr>
<td>Administrator Account</td>
</tr>
<tr>
<td>Administrator Password</td>
</tr>
<tr>
<td>Domain name</td>
</tr>
<tr>
<td>Server LAN IP</td>
</tr>
<tr>
<td>Server’s OS</td>
</tr>
<tr>
<td>Server’s Role</td>
</tr>
<tr>
<td>• Domain Controller (DNS,DHCP)</td>
</tr>
<tr>
<td>• Exchange Server</td>
</tr>
<tr>
<td>• SQL Server</td>
</tr>
<tr>
<td>• File Server/Print Server</td>
</tr>
<tr>
<td>• Web Server</td>
</tr>
<tr>
<td>• Blackberry Server</td>
</tr>
<tr>
<td>• Application Server</td>
</tr>
<tr>
<td>Hard Disk Size</td>
</tr>
<tr>
<td>Number of Hard Drives</td>
</tr>
<tr>
<td>Fault Tolerance (Raid Configuration)</td>
</tr>
<tr>
<td>• Raid 0</td>
</tr>
<tr>
<td>• Raid 1</td>
</tr>
<tr>
<td>• Raid 5</td>
</tr>
<tr>
<td>• Raid 10</td>
</tr>
<tr>
<td>Misc. Information</td>
</tr>
</tbody>
</table>
## Firewall

<table>
<thead>
<tr>
<th>Hardware/Software</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Make/ Model</td>
<td></td>
</tr>
<tr>
<td>LAN IP Address</td>
<td></td>
</tr>
<tr>
<td>WAN IP Address</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Remote Management (Enabled/Disabled)</td>
<td></td>
</tr>
<tr>
<td>Ping (on/off)</td>
<td></td>
</tr>
<tr>
<td>VPN(s)</td>
<td></td>
</tr>
<tr>
<td>Open Ports</td>
<td></td>
</tr>
<tr>
<td>NAT’ing Outside/Inside</td>
<td></td>
</tr>
</tbody>
</table>

## LAN Info

<table>
<thead>
<tr>
<th>LAN Subnet</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server’s IP</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Switch IP</td>
<td></td>
</tr>
<tr>
<td>Switch Name</td>
<td></td>
</tr>
<tr>
<td>Switch Make/Model</td>
<td></td>
</tr>
<tr>
<td>Switch Warranty</td>
<td></td>
</tr>
</tbody>
</table>

## Anti-Spam

<table>
<thead>
<tr>
<th>Anti-Spam Solution</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>
### Antivirus / Antispyware

<table>
<thead>
<tr>
<th>Virus Protection Software</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus Software</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Expiration Date</td>
<td></td>
</tr>
<tr>
<td>Spyware Protection Software</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Expiration Date</td>
<td></td>
</tr>
<tr>
<td>Misc. Information</td>
<td></td>
</tr>
</tbody>
</table>

### Backup

<table>
<thead>
<tr>
<th>Backup Software and Version</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Schedule</td>
<td></td>
</tr>
<tr>
<td>Backup Device (Type &amp; Model)</td>
<td></td>
</tr>
<tr>
<td>Number of Backup Tapes or Storage Available</td>
<td></td>
</tr>
<tr>
<td>Remote Backup/Vendor Name</td>
<td></td>
</tr>
<tr>
<td>User Account</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

### User Accounts

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Network Device Inventory

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Make &amp; Model</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Printers & Peripherals

<table>
<thead>
<tr>
<th>Type &amp; Model</th>
<th>Share Name</th>
<th>Physical Location</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix D: Service Delivery Email Template Sample

—REPLY above this line to respond—

**SYSTEM ALERT - SERVICE TICKET NOTIFICATION**

[contact first name]   [contact last name]:

We have received a SYSTEM ALERT from your computer and ticket number [srnumber] related to “[srsummary]” has been created automatically for this issue. If you would like for COMPANY NAME to address this issue please reply to this email indicating your desire for us to resolve the issue on your behalf. A technician will be scheduled to complete the task then follow up with you. If you wish to not have the issue addressed then simply ignore this notification and do not respond.

Please reference the details listed below for more information; the provided chart gives an explanation of each alert and how it impacts your Networks Security, Performance and Dependability and is organized by category, frequency and a description of the alert to help with your decision making process.

Regards,

Your IT Support Team

800-123-4567

You can check the status of your Service Ticket in the Customer Portal.

My Company | Address | City, State Zip | ©2012 My Company. All Rights Reserved.
Appendix E: Help Desk Incident Management Flowchart

Problem Management/Tracking Process in a Three-Level Help Desk Organization

Customer Discovers Problem

Customer Contacts Help Desk (Phone, Fax, E-mail)

Problem Logged In & Ownership is Assigned

Level One Technician Attempts to Solve Problem

Resolution at Level One?

Problem Owner Verifies Customer Satisfaction

Problem Record Marked Closed

Update Problem Record / Notify Problem Owner of Solution

Database

Provide Customer with Tracking # / Provide Estimate of Time of Resolution

Database Updated

Resolution at Level Two?

Change Management / Recording of New Solution in Database

Database

Resolution at Level Two?

Level Two Technician Attempts to Solve Problem

Problem Passed to Level 2 Technician

Resolution at Level Two?

Level Three Technician Attempts to Solve Problem

Problem Passed to Level 3 Technician

Resolution at Level Two?
About the Authors

Kevin Gibson

Kevin Gibson has over 20 years of technology experience in developing and managing enterprise information systems, including four years overseeing service and product development for a technology solution provider (TSP) in the Metro Atlanta area. In the early days, Kevin was involved in his own technology-based business venture that began as an Internet Service Provider (ISP) and was acquired by MindSpring in November 1999. Following the acquisition, Kevin continued to focus on the small and medium business segment by way of providing consulting and systems management to small businesses around the Southeast, which led to his company merging with Atlanta Technology Force (ATF) in February 2008. He also spent six years working with the Georgia Department of Transportation where he oversaw the department’s infrastructure of 5,000 users prior to merging with ATF.

Kevin is currently a Transformational Services Strategy Director for ConnectWise. Prior to this role, he was a Senior Product Manager for ConnectWise Automate where he was responsible for driving key ConnectWise Automate technologies, including availability management, ConnectWise Automate Ignite®, professional services automation (PSA) integrations and MyOffice integration.

He is a Microsoft Certified Systems Engineer, Microsoft Certified Systems Administrator, VMware Certified Professional and holds a Bachelor’s degree in Business Administration from Georgia State University.

Vernon Southmayd

Vernon Southmayd, Director of Product for ConnectWise Automate, has been a principal in multiple computer-related companies over the past 28 years. He has watched the business models in the computer industry change from reseller to value added reseller and to today’s MSP model. He believes that Automate is uniquely positioned to help our partners become more efficient and provide more value to their clients by leveraging automation.

Vernon is responsible for understanding how our partners use Automate in their business each day and works with our product management and development groups to improve that experience. He is focused on building out Automate as an IT Service automation platform that empowers our partners to create automation that exceeds their client’s expectations.
About ConnectWise

ConnectWise transforms how technology solution providers successfully build, manage, and grow their businesses. Offering a comprehensive set of award-winning solutions that deliver a seamless, simple user experience, ConnectWise gives its partners the ability to increase productivity, efficiency, and profitability.

Just as importantly, ConnectWise’s relentless commitment to innovation and unparalleled passion for partner success assure its partners have comprehensive business support through every step of their journey. Today, more than 120,000 users in over 50 countries take advantage of the competitive edge that comes from ConnectWise solutions and its powerful network of ideas and experts.

For more information, visit ConnectWise.com or call 800-671-6898.