MSP Service Management Process
# Table of Contents

Table of Contents ........................................................................................................... 2  
Document Overview ........................................................................................................ 4  
Service Management Process Prerequisites ................................................................. 4  
Service Management Processes Defined .......................................................................... 4  
  Configuration Management ........................................................................................... 5  
  Configuration Management Defined ............................................................................ 6  
  Configuration Items in Detail ....................................................................................... 6  
  Establishing a Baseline ............................................................................................... 7  
  Maintaining Accurate Configuration Information ..................................................... 8  
  Ensuring Data Accessibility ....................................................................................... 8  
  Configuration Management Reporting ..................................................................... 9  
  Incident Management ................................................................................................ 9  
  Call Detection and Recording .................................................................................... 11  
  Classification and Prioritization ................................................................................ 11  
  Initial Support ......................................................................................................... 13  
  Update Customer Ticket ............................................................................................ 13  
  Document Resolution ............................................................................................... 14  
  User Feedback .......................................................................................................... 14  
  Incident Reporting ................................................................................................... 14  
  Problem Management ............................................................................................... 15  
  Problem Control ....................................................................................................... 17  
  Error Control ............................................................................................................ 18  
  Major Problem Reviews ............................................................................................ 18  
  Change Management ............................................................................................... 19  
  The Instigators of Change ......................................................................................... 19  
  The Change Management Process ........................................................................... 19  
  Availability Management ......................................................................................... 21  
  Availability Requirements ......................................................................................... 23  
  Availability Design .................................................................................................... 24  
  Managing Availability .............................................................................................. 24  
  Capacity Management .............................................................................................. 25  
  Capacity Requirements ............................................................................................. 26
Capacity Design............................................................................................................................................. 27
Managing Capacity........................................................................................................................................ 27
IT Service Continuity Management ............................................................................................................. 27
  IT Continuity Planning ............................................................................................................................ 29
  IT Continuity Implementation .................................................................................................................. 31
Manage the IT Continuity Plan .................................................................................................................... 31
Measurement and Improvement .................................................................................................................. 31
Document Overview

The Service Management Process document is designed to provide a structured approach to supporting multiple managed services customers in a scalable, predictable and cost effective manner. This document serves as the core repository of that process documentation.

Service Management Process Prerequisites

The Service Management processes are not truly called into play until after the customer has entered into a managed services engagement with the MSP. The fundamental reason for this is that, as the name implies, the service level agreement (SLA) defines the level of service that the customer is expecting and that the MSP has committed to provide.

This process also assumes that the NOC reconfiguration process has been completed. This is an important step as configuring the service desk tools to reflect the service commitments within the SLA is fundamental to a successful engagement.

Service Management Processes Defined

The network operations center (NOC) makes use of a number of processes, as shown in Figure 1, as part of the day-to-day activities related to managing multiple customers in a managed services environment. The processes defined in this manual have been developed based on the ITIL (IT infrastructure Library) model as they specifically apply to an MSP servicing multiple SMB customers.

The processes defined within this document include:

- Configuration management
- Incident management
- Problem management
- Change management
- Availability management
- Capacity management
- Business continuity management
As shown in Figure 1 there are other processes that relate to the service desk, most notably the service level management process (SLM). However these processes are not NOC operational processes they are only referenced within this document. Please review MSP Service Level Management document for more details.

**Configuration Management**

The purpose and point to configuration management is to develop and maintain an accurate representation of each customer’s IT infrastructure. As clearly identified in Figure 1 the information maintained by the configuration management process is critical to the effective and efficient execution of every other service delivery process. When one considers that over 60% of all incidents are caused by a change in configuration\(^1\) rather than an actual failure, it becomes clear why this process is key to an effective managed services organization.

---
\(^1\) EMA Associates
Configuration Management Defined

Configuration management is the identification, recording and reporting of IT components. While operationally configuration management is similar in nature to asset management, it differs greatly in purpose and depth. Asset management is an accounting function, whose primary aim is to effectively identify and record the corporate IT assets with the purpose of managing the lifecycle and usage of hardware and software within the customer organization.

Configuration management is an IT function, whose primary aim is to identify, record, and maintain a detailed description of the IT infrastructure, including the relationships between configuration items (assets) with the purpose of leveraging that information to optimize the efficiency and effectiveness of all other service delivery processes.

Configuration Items in Detail

A configuration item (CI) is an element of the IT infrastructure that can be managed. At the top level this includes mission critical business services such as email and web services. These top-level CIs can be broken down into lower level configuration items such as servers, routers, switches and applications. This continued decomposition of the configuration items can continue down to the component level. The challenge becomes managing the volume of the configuration items and the relationships.

Taken to the extreme, micro-managing the configuration items within an IT infrastructure becomes more costly (both in terms of time and the tools to manage it) then it’s worth. The N-able recommendation is to manage configuration items at the following level:

- System SKUs (or baselines) – every system defined by the same SKU is identical with respect to the hardware profile
- Application SKU – similarly every system defined by the same application SKU has the identical operating system and application profile
- Relationships – There are two key types of relationships that must be documented and maintained:
  o Physical - A topological diagram that illustrates how every device plugs into the network
  o Logical – A series of diagrams that illustrate how devices (and other business services) combine to create business services
Note: Understanding the logical implications of a device is critical to understanding the appropriate risk and priority of the system. Example: The networking devices are an obvious example of components that interact with every business service. When a core router fails, every business service is impacted.

Ideally these SKUs would apply across customers, allowing the MSP to minimize the number of profiles under management. This becomes much more feasible in higher level programs (fixed fee, hardware as a service and utility) where the MSP has sufficient level of control over the hardware choices being made by the customer – but in almost all cases new customers will have unique legacy equipment that must be accommodated within the process.

Not only does this simplify the task of managing a wide range of devices and applications, but it will dovetail into other recommended operational management practices such as:

- **Imaging** – Imaging is a way to create a snapshot of an operating system and applications. Most MSPs that leverage this technology create a library of images of freshly installed operating systems and applications. Once created they can apply that image to a new system in a very short period of time – thus reducing the cost of deployment and decreasing the opportunity for human error.
- **Monitoring Templates** – The most effective means of quickly deploying monitoring services to a system. By creating templates that correspond to system and application SKUs the MSP is able to further optimize the deployment of the monitoring services.
- **Business Continuity** – Established SKU baselines, the above described imaging combined with an effective data backup and recovery strategy lays of solid groundwork for a business continuity plan – where the entire IT infrastructure could easily be replaced from the ground up if required.

**Establishing a Baseline**

When an MSP begins to work with a new customer, there is no existing knowledge of the IT infrastructure. So the obvious first task is to develop the baseline information about the customer infrastructure. This can be broken down into two major steps:

- Data collection
- Data organization

Data collection occurs as part of the customer infrastructure audit (network, security, regulatory compliance) – for details on this process please review the N-able MSP Deployment Process document. If done correctly the MSP should have all of the necessary information required when populating the configuration management database.
The organization of that data is a key step to making the information manageable. The device and application profiles must be documented in terms of SKU information – consistent with the MSP practice. As a best practice the MSP should take images of every SKU as soon as possible (once the contract has been signed).

**Maintaining Accurate Configuration Information**

Like as not the customer IT infrastructure is in a continuous state of change, either as a result of a problem discovered with the existing configuration or in order to extend the IT infrastructure to deliver new value to the customer. With respect to configuration management it is *critical* to adopt a process where all planned changes to the customer infrastructure (emergency and scheduled) are reflected in the change log associated to a device. In this manner a device will have a reference to a set of SKUs that will define the *baseline* configuration and a change history that will document *how* the configuration of that device has deviated from the original baselines.

In theory it should be possible to maintain a configuration database (baselines + change logs) that accurately reflect the profile of every component of the customer infrastructure. The practical MSP doesn’t rely only on the change process to maintain the configuration information. Periodically it is important to vet the assumed configuration information against the actual profile of the systems in production. Useful tactics include:

- **N-central Change Monitoring** – Define the hardware baseline of each system such that it matches the records in the CMDB (refer to N-central documentation for details) and initiate change monitoring – N-central will automatically notify the MSP in the event of a change to the hardware profile, which can then be compared against the forward schedule for change (see change management) and the configuration management system to determine if this was a planned change.
- **N-central Application Monitoring** – Similarly by determining the application baseline of a system the MSP can be instantly notified if unauthorized applications are installed on the system.
- **Periodic Audit** – A physical audit of the infrastructure must be conducted periodically. Depending on the nature of the engagement, this may be a pay-for service or incorporated into the managed services program. If it is incorporated into the program, the MSP must account for the cost of the audit (time) in the overall program cost.

**Ensuring Data Accessibility**

The purpose of maintaining the detailed information is to make it available in a read-only format to other service management processes and functions such as the service desk (incident management), the NOC Operations and Field Techs. Given the fact that
not all of the people that need to see this information will be located within the MSP office, consideration must be given to making sure that the data is available to all who need access to it, and who are authorized to access it.

Configuration Management Reporting

The focus of configuration management is on managing information on the IT assets in order to facilitate effective stewardship of those assets. Intrinsic to this mandate is facilitating effective planning (in conjunction with the customer) as well as illustrating inherent IT transparency. N-able supports both of these activities through the N-central infrastructure, with the following reports:

- Application Compliance by Application
- Application Compliance by Device
- Asset Site Report
- Detailed Asset Report (should only be generated during configuration audits)

Incident Management

When a customer is experiencing an issue, whether it’s a network outage, or an inability to perform an action because they don’t know how to use the system, they want an expedient resolution to their problem. Restoring a customer to operational status as quickly as possible is the purpose of an incident management process. This process defines how and where incidents originate, escalation points and definitions of categorization and prioritization.

From the perspective of being responsive to a customer’s needs, incident management is probably the most critical of all IT service support services.

Incident management is comprised of the following activities:

- Call Detection and Recording
- Classification and Prioritization
- Initial Support
- Escalation (if applicable)
- Document resolution
- Request user feedback
Additionally the incident management process interacts with the following other service management processes:

- Service level management
- Problem management
- Configuration management
- Service Request management

Figure 2: Incident Management Process
**Call Detection and Recording**

The incident management process reacts from some stimuli within the customer environment. Depending on the infrastructure in place, the nature of this input could be:

- A customer call into the service desk
- An email into the service desk
- An auto-populated ticket created from the MSP’s web portal
- An auto-populated ticket created by a remote monitoring and management (RMM) system

Depending on the nature of the input, the technician may or may not have to create the actual case within the MPS’s PSA or ticketing system. In all cases however, the technician will have to establish ownership of the ticket usually by accepting it himself or herself, or sometimes by assigning it someone else.

The most basic function of an RMM solution is to monitor the up/down status of IT services within the customer infrastructure. Alerts based on these *availability* services are indicative of a business impact from IT failure and as such are of a higher priority than predictive failure or capacity based alerts. N-central services that reflect availability include:

- Connectivity
- TCP/IP based services (stock or custom)
- Process based services (Proc or custom services)
- Log analysis based services
- Windows event log service
- Syslog based events

Some users may (intentionally or otherwise) log multiple cases through a single incident. For logistical management and accurate tracking it is important to separate each incident or question or service request into a separate incident – even if the customer is making all of those requests on the same phone call.

**Classification and Prioritization**

Users will contact the service desk for any number of reasons; the next task of the service desk technician performing the incident management function is to define the *type* of call, which will be one of:
Service disruption – The call pertains to an incident which is defined as an abnormal condition of customer’s infrastructure that is impacting the normal delivery of IT service

Service request – The customer is calling for a move/add/change/delete type request

Consumables request – Materials such as printer toner

Information request – how to type queries

If the nature of the call is about an incident, the service desk technician must prioritize the case. The purpose of prioritizing the tickets is to allow the efforts to be conducted according to a triage mentality rather than simply first come, first serve. The priority of an incident should be based upon three separate elements:

- Impact: How many users are affected
- Urgency: How debilitating is the nature of the incident
- SLA: What is the service level objective in this case

On the basis of these two factors the service desk should be able to assign a priority to the incident. Standard priorities include:

- Blocker – A blocker issue prevents a user from performing a core component of their job. A blocker incident has no workaround
- Critical – A critical issue prevents a major system to be used in an effective manner. There is a workaround for a critical
- Normal – A normal incident detracts users from their ability to use the system. There is a workaround
- Minor – A minor issue is an issue that can be worked around, and dealt with during a scheduled maintenance period

In addition to the priority that is assigned to an incident every case should have a status that indicates where it is in its lifecycle. The parameter, often called the workflow position may include:

- New
- Accepted
- Scheduled
- Assigned/Dispatched
- Work in progress
- On hold
- Resolved Closed

In the case of incidents the service technician should also document as much detail as to the nature of the issue as possible including symptoms, manifestations, ways to reproduce, whether the issue is continuous or intermittent, etc. The key is to collect and document as much information as possible.
If the customer is calling regarding a service request, the appropriate information should be collected and passed on to the service request process.

Note: The defined priorities as well as the workflow parameters should be configured directly into the PSA/ticketing solution. This requires that the system support custom objects or at a minimum configurable lists.

**Initial Support**

The objective of initial support is for the service desk technician to resolve the incident remotely if possible. In order to accomplish this, the technician will have to use all available information including the customer description of the event, information collected from the RMM system as well as the details of the affected systems from the configuration database.

**Update Customer Ticket**

Every action, resolution attempt or troubleshooting step must be documented within the case history including any output or response. Not only should the descriptions of the activities be documented, but which technician updated the case and at what time and date was the case updated. This provides several benefits to the customer and the MSP:

- Relives the customer from having to work with a specific technician throughout the lifespan of their incident. The user can contact the service desk with a ticket or case number, and any technician can pick up where the last technician left off.
- Clear case history – for reporting and service desk optimization, the service desk has a complete history of all actions taken.
- Governance and follow up – The detailed accounts of service desk activities help ensure compliance with corporate governance best practices.

If the level 1 service desk can’t resolve the incident, then the case needs to be functionally escalated to the NOC operations team (level 2) as part of the problem management process. If the customer becomes irate for whatever reason, then the case may need to be hierarchically escalated to the service desk manager or the on duty supervisor.

Note: The service desk (level 1) is responsible for customer contact. This means that even if the level 1 technician escalates the incident to level 2, they still own the ticket and as such are responsible for tasks such as providing case status updates to the customer and collecting additional information from the customer if requested by level 2.
**Document Resolution**

Once a solution for the incident is found, either because the service desk technician was able to provide a solution or because the problem management function provided a resolution, the case must be resolved. The case log must be updated with a description of the resolution – or a link to the described problem resolution and the workflow position of the case moved to ‘resolved’

**User Feedback**

Once the case is resolved, the customer must be contacted to determine their satisfaction with the resolution. Ideally the only person that can close a ticket *is the user that opened it.* In practice the MSP will have to develop policies that accept the fact that some customers may never respond to the feedback request. To accommodate this, some organizations include two different closure states within the workflow position:

- Closed by customer
- Closed by MSP

In this case the relative percentage of cases closed by the customer vs. the number closed by the MSP becomes a metric of customer satisfaction.

**Incident Reporting**

Incident management as a process has a direct bearing on the availability of the customer systems. Incident reports *should* be used internally to support process improvements as well as externally to illustrate. Incident reporting is ideally driven from the PSA/ticketing solution as this system manages all incidents regardless of the source. Key reporting information includes:

- Number of incidents in the reporting period divided by priority
- Source of those incidents (N-central, phone, email, web)
- Mean time to recovery vs. objective
**Problem Management**

If incident management is about resolving customer issues quickly, then problem management is about identifying the underlying cause of one or more incidents and making recommendations to improve the ongoing stability of the infrastructure – by either producing a workaround and/or a solution for the problem. By the very nature of this process problem management is both reactive and proactive at the same time. By solving the problems that are causing a current incident, problem management is contributing to reactively supporting customers. By correcting the underlying problem or weakness within the infrastructure, thus preventing *future* incidents of a similar type, problem management is contributing to the proactive support of the customer as well. The problem management process illustrated in Figure 3 divides activities into two main areas of focus; problem control and error control.
Figure 3: Problem Management

PSM/Ticketing system (Incident/Problem/Error Database)

Tracking and Monitoring of Errors

Tracking and Monitoring of Problems

Error Management

Problem Management

Inputs to Problem Management

- Detailed analysis (Root Cause Analysis)
- Problem management (Configuration Management)
- Incident management (Incident Management System)
- Knowledge Management (Knowledge Base, Tool Support)
- Change Management (Change Control)
- Test Management (Test Cases, Test Environment)
**Problem Control**

According to the ITIL definition, a problem is the unknown cause of one or more incidents. The source of incidents in the MSP model could be:

- Incident management process – These would include all incidents that impact the customer
- Predictive failure events (RMM) – If configured properly the remote monitoring component of the MSP toolset will collect information that indicates conditions leading to a business impacting failure
- Industry information – New viruses, spyware and exploits will continually be developed. If not checked these may cause a business impact.

While the activities of problem control will help to prevent future incidents, it is more closely aligned with incident management, as such is focused on diagnosing problems (what device is at fault) and developing a workaround for the service desk if possible. The primary components of problem control are:

- Problem identification and recording, which includes
  - Routine procedure – some activities require escalation, although they may be routine in nature.
  - Error matching – determine if the incident matches a known error, if so update error and incident records appropriately
  - Problem matching – determine if the incident matches a known problem, if so update the incident and problem record accordingly
  - Create new problem – only if the incident doesn’t match a known error or known problem
- Problem classification and prioritization – New problems must be classified in a similar fashion to incidents. As such the technician must define:
  - Category – Separated by domain expertise (hardware, network etc)
  - Impact – The impact on the business (how many critical business services, or users are affected)
  - Urgency – The depth of impact to the business services. Determination of urgency should include a review of:
    - Can users continue to function?
    - Does a workaround exist?
    - What about a delay of resolution?
- Problem investigation and diagnosis

In order to be both useful and relevant problem control must not only focus on solving the problem, but also on making the resolution information available and accessible to everyone that needs it. Examples of output from this process include:

- Known errors
- Indexed description of problem/resolution/workaround – Very few problems are new. The reason that they get escalated to problem management is because the service desk can’t find any relevant information. A well documented and indexed case (i.e.: searchable) will help reduce the number of incidents being escalated**
- Update of all associated cases
- Knowledge base articles – Where a workaround or fix can be implemented by the user, the information should be published to the knowledge base in the customer resource center, especially if the objective is to reduce the traffic to the service desk by encouraging self service
- Continuous training to the service desk

If the problem control process is working properly there will be a large amount of data available regarding problems, solutions and workarounds, some relevant and some out of date. An additional challenge becomes maintaining all of this information as an abundance of out-dated information will make searching the database far more challenging. Therefore it becomes important to periodically ‘scrub’ the database to remove articles on problems that are no longer relevant.
Error Control

Once a problem is diagnosed and provided with a workaround it ceases to be a problem and becomes a known error. The focus of error control is to systematically eliminate known errors. This would be accomplished by implementing a change under control of change management (more on that later) if and when it is feasible and cost justifiable to do so. The steps involved in error control include:

- Error identification and handling
- Error assessment
- Record error resolution

Errors are generally identified in one of two ways:

- A problem in a customer’s production environment is diagnosed and a workaround found – thus elevating to an error status
- An error is identified within the MSP’s lab environment.

In the latter case (error detected in a lab environment) the MSP would evaluate the impact of the error. If the error is of sufficient magnitude the deployment of the affected system may be halted until a workaround can be devised. If the error is manageable than the MSP will release the affected system, ensuring:

- Release notes include details of the known error
- The service desk is aware of and trained on the workaround for the known error
- The customer is aware of and has signed off on the deployment of the system knowing that the error is present

The normal outcome of the error control procedures is a change request. A change request describes in detail the nature of the change being requested, the reasons for the change as well as information required to support a business case

- Cost of the change
- Risks associated to the change
- Ongoing cost of not implementing the change

Major Problem Reviews

Periodically a major problem will occur at a customer location that will test the capabilities of the MSP. After the problem has been handled, the MSP has an opportunity to improve their operations through an exercise called the major problem review. The focus of the major problem review is to identify:

- What was done right
- What was done wrong
- What are the top priorities for improvement
- How can those procedural changes be implemented

It is important to note that the focus of the major problem review should not be limited to the problem management process but also include practices that may have caused the problem. Since the MSP is responsible for the assessment, deployment, and management of the customer systems, the major problem review should also ask the questions:

- Did we introduce the problem?
- Could we have caught the problem through a more effective assessment process (pre-sales)
- Could we have caught the problem through a more effective monitoring and management approach (post sales)

In this way the MSP is able to continually improve the operational behavior of all aspects of their service delivery.
**Change Management**

Change management is a service support and delivery process designed to minimize the business impact of change. While change is inevitable in the IT world, the truth is that the majority of IT failures can be directly related to a system or application change within the customer infrastructure. The obvious solution is to not change anything, but since other processes like problem management demand change in order to solve existing issues, the key lies in balancing the benefits of change vs. the cost of change and taking all appropriate measures to minimize negative impacts due to change.

**The Instigators of Change**

From an IT management perspective change equals destabilization of an existing ecosystem. With this in mind it is beneficial to understand where change within the IT infrastructure originates. Change can be traced to the following processes and activities:

- **Problem management** – As part of the normal process of eliminating weaknesses within the customer infrastructure
- **Capacity management** – As the customer business grows, there will be new demands on the IT infrastructure that will eventually impact the quality and availability of the service
- **New service delivery** – As the needs of the customer business grow and evolve to include new IT services, the impact of those services on the existing infrastructure need to be accommodated

Note: Implementing a change within the customer infrastructure is a project. Therefore although we discuss the process of change management, it is important to understand that this process is used in tandem with an effective project management process.

**The Change Management Process**

The change management process focuses primarily on the roles of the ‘change manager’ and the change advisory board. The change manager is an administrative role, designed to manage the approval (or decline) of changes through the change management process. The change advisory board (CAB) is a group of senior stakeholders that have the authority to make go/no go decisions on major changes. The individuals that would belong to a CAB would include:

- Account manager
- Service manager
- Representative of the customer
The major steps for a typical MSP change management process, as shown in Figure 4, include:

- **Request Filtering** - Some changes will simply not provide anywhere near enough value to justify the cost. The change manager can filter these change requests immediately.

- **Prioritization** - Generally changes will either be urgent (critical problem with no work around) or they will be standard. The change manager must use the information provided in the request for change to determine the priority and then act accordingly.

- **Determine Scope of Change** - The above model illustrates two scope models (minor and major) where the change manager has authorization to approve minor changes and the change advisory board (CAB) must approve major changes. Depending on the size of the MSP, the size of the customer’s they engage with, regulatory implications etc, there may be many more scope models that include further levels of approval – potentially all the way up to the customer’s board of directors. The scope of the change will be determined by evaluating:
  - The level of comfort with the tasks associated to the change
  - The cost of the change as it relates to the pre-authorization of each scope model
  - The risks (technical and business) associated to the change

- **Circulating Change to Approval Board** - If approval needs to be provided by a higher level body than the change manager (CAB, or other) than the change manager, with the assistance of the change request author need to brief the approval board on all aspects of the change.
- Approval Board Assessment – The CAB (or other approval board) will assess the cost, impacts and risks of the change and make a decision on the change.
- Notify CAB – If the change falls within the authority of the change manager, then the CAB will be simply notified of the change. Common practice is to notify the CAB in a digest format of all of the changes that have occurred during a predefined reporting period.
- Denied RFC – If the RFC is unauthorized, the change manager will update the RFC with the appropriate information as to why it was declined. This allows the author (if they should so choose) to update the RFC and re-submit.
- Update Forward Schedule of Change – Once approved the change manager adds the change to the forward schedule of change.

Note: The forward schedule of change (FSC) is almost exactly like the change log –except that it describes changes that are going to occur rather than changes that have occurred.

- Plan the change – Including:
  - Change specification – depending on the scope of the change a specification may need to be developed that describes the planned implementation of the change
  - Rollback plan – Every planned change needs to have a rollback plan in case of emergency
  - Project Plan – Once the complete scope of work is know a final project plan must be developed that can be communicated to the customer – may also require an update of the FSC
- Test the change – The change must be tested in a lab environment prior to deployment in production. Ideally the change is tested by somebody other than the developer of the change.
- Archive the change – For the purposes of rapid deployment (either for new deployments or IT continuity planning) it is useful to have an archived image of the new configuration
- Implement the change – The change is implemented in the customer location.
- Implement Rollback – If the change is unsuccessful, the systems must be rolled back to the previous configuration
- Update change log – In order to keep the CMDB up to date, the change must be moved from the FSC to the change log
- Review the Change – As an exercise to improve processes

Additionally the MSP requires an urgent change process to deal with critical changes that must be pushed through the process quickly in order to restore service to high priority services– without sacrificing control of the process. The process is effectively identical with the exception of the service manager calling an all-hands-on-deck condition where everybody that is required as part of the process is expected to be available on an as-needed basis. Operationally the key (different) elements to an urgent change process include:

- Providing the change manager with the decision framework with which to identify an urgent issue
- Identifying the key individual required in the event of an all-hands-on-deck situation (including backup personnel)
- Ensure the service manager has contact information for all key individuals

**Availability Management**

Fundamentally all of the service delivery processes such as incident and problem management focus on maximizing IT availability. Availability management differs in that it looks at the design, implementation and management of services in order to achieve the right level of availability to satisfy the business requirements – as defined within the service level agreement, all within the defined cost structures. Operationally, availability management applies to the managed service provider in the form of considering the availability impacts when constructing the customer’s complete IT plan. By that definition, availability management impacts a number of service delivery and service support activities.
Availability Management can be considered in three major areas; the work that must be done in order to understand the costs of providing the customer the required availability, which of course must be done before the contract and service level agreement for fixed fee managed services is complete; the work that must be done to build and IT infrastructure that will support the availability requirements, which must be defined prior to the finalization of the agreements; and the work that must be done to support the required availability, once the managed services engagement is under way.

Note: While availability design activities are generally conducted in a presales mode, anytime there is a significant change to the requirements for availability (new IT services, significant change in headcount, etc) the MSP must review the availability design and service level agreement with the customer – potentially resulting in a new or amended SLA.

As shown in Figure 6, Availability management boils down to balancing the requirements for availability, the cost of architecting for availability and the cost of managing availability. To a certain extent any two points of the triangle can be fixed – as long as the third point is free to be move (within limits). So the cost of architecting and managing availability can be predefined (within a reasonable range) as long as the requirements availability requirements remain flexible. Conversely, the availability requirements and the cost of managing availability (again, within reasonable ranges) can be predefined as long as the cost of architecting for availability is subject to change.
The first and most important step in building an IT plan that matches a customer’s availability requirements is to *understand* what those availability requirements are. This is done in a presales mode as part of the in-depth Business Discovery/Needs Analysis in conjunction with the network audit (please review the associated documents for a complete description of those process). In general the business discovery/needs analysis should uncover:

- The prioritized list of mission critical business services
- Revenues supported by each IT service
- Productivity supported by each IT service
- Business impact requirements for each mission critical IT service
- A logical diagram that illustrates the physical configuration items that support each business service

The above information is combined with the MSP’s requirements for supportability to produce a complete picture of the infrastructure that must be put in place in order to support the customer’s availability requirements in a fixed fee managed services model.

Since the typical customer probably hasn’t put much thought into the availability requirements of the IT infrastructure it is incumbent upon the MSP to *help* the customer understand what those availability requirements truly are. This includes consideration for availability models (24/7, business hours, etc) as well as helping to build a model with the optimal levels of availability.

The cost of downtime can be defined based on revenue generation per IT hour and the cost of productivity per hour – both of which are impacted to varying degrees when mission critical IT services fail. Conversely the cost of achieving increasing levels of availability can be quantified by the cost to implement appropriate infrastructure combined with the cost to manage that infrastructure. It generally accepted that the costs for availability increase exponentially as the availability requirement *nears* 100% (where it is impossible to achieve 100% availability). At some point the total cost of availability outweighs the tangible benefits of availability.
In practice, a reasonable availability target will be defined as part of the business discovery/needs analysis phase of the engagement model. Once the MSP returns to the customer with the key findings and infrastructure upgrade proposal there should be an opportunity to review the availability requirements, which will in turn trigger a revision of both the availability design costs and the availability management costs.

**Availability Design**

As the requirements are effectively defined the MSP designs the ideal infrastructure that achieves the appropriate balance between availability by design (upfront costs) vs. managed availability (ongoing costs) in order to achieve the customer’s availability needs.

What ultimately comes out of these activities are:

- An agreed upon set of availability metrics which will become part of the SLA (as such these activities are also part of the Service Level Management process)
- IT architecture & designs which will be presented as key findings, including a gap analysis between the required infrastructure and the current infrastructure, prioritized in terms of project phases (immediate, mid-term and long term) including costs for each project phase.
- Disaster recovery plans that illustrate how the MSP will recover the above designed infrastructure in case of disaster – keeping in mind that there are different levels of disaster, the complete plan must account for all contingencies (as part of Business Continuity Process as discussed later in this document)
- Managed services costs

**Managing Availability**

Once the availability targets are set, the SLA signed and the upgrade projects complete (at least the initial upgrade project), considerations move towards managing the IT infrastructure to achieve the desired availability within (ideally well below) the defined cost structure. The MSP should expect higher than normal levels of incident and problem management activities early on in the engagement as the infrastructure stabilizes, followed by leveling of activity and associated costs. Operationally, this supported through N-central monitoring of the key indicators of availability (Section: Incident Management) for each device that supports a mission critical IT service.

The process of managing availability at this point interacts directly with incident, problem, change and IT business continuity processes as these are the core vehicles by which the IT infrastructure is supported by the MSP. Availability management as a process becomes
focused on monitoring the inputs that affect availability (monitored availability, incidents, problems etc) as well as the cost for service delivery and working to increase the customer’s availability levels and/or decrease the overall cost of supporting those availability levels and finally on providing appropriate availability reports to the customer to illustrate the value of the provided service, and to help plan for changing availability requirements. Reports that can be provided from the N-able toolset (N-central and N-compass) to support availability management include:

- Availability Aggregated for One Service on One Device (N-central) – Should be generated for each business critical service
- Availability of Multiple Services on One Device (N-central) – Select the services that support the business critical service
- Incident Summary Report (N-central) – While not all incidents affect availability, the metric will serve as a barometer to activity
- Network Health Overview (N-compass) – Not limited to availability, but does include a key section on network availability
- Application Availability (N-compass)
- Downtime Cost Impact Report (N-compass)

As with all customer facing reports, these reports should be delivered to the customer by an analyst. The report analysis is a key element to interpreting the reports into information that affects the customer’s business – which is a significant component to the value of the managed services program.

**Capacity Management**

Mission critical IT services are implemented with a capacity to fulfill a certain amount of work. As these services are considered in terms of the physical devices and applications that make up those services we truly mean the capacity in the following areas:

- The capacity to process data – which may be impacted by:
  - CPU (number, speed and type)
  - Memory (amount and type)
  - Disk I/O speed
  - System bus speed
  - Application processing performance capacity

- The capacity to share/move data
  - The local network capacity
  - The I/O capacity of the endpoint devices (servers and workstations)
  - The Internet throughput (affected by connection speeds and ISP congestion)
  - Application I/O capacity

- The capacity to store data
  - Local file size
  - Shared file size
  - Storage model

The objective of capacity management is to ensure that the customer has the correct amount (not too little, not too much) of the above-defined capacities – understanding that the customer’s business is dynamic and that the requirements for capacity will change over time as the customer increases the use of technology within their operations, the size of the customer and their customer base grow, and simply as the amount of data that is generated (and must be maintained) increases through normal operations.
As shown in Figure 8 the activities associated to capacity management can be considered in terms of three high-level categories - business capacity management, service capacity management and resource capacity management and like availability management, should be considered in terms of three separate areas:

- Capacity requirements
- Capacity design
- Managing capacity

**Capacity Requirements**

As with other service delivery disciplines the MSP must understand the overall requirements for capacity before setting out to design a capacity plan. The inputs to the capacity requirements may include:

- **Current capacity** – The current capacity utilization levels, combined with an assessment of whether or not the customer deems that level of capacity to be achieving their current requirements
- **Business requirements** – The business requirements can be sub-divided into several important areas:
  - Business plan – Planned changes to headcount, business initiatives etc may have a predictable affect of capacity that can be planned for in advance
  - Regulatory implications – The business may (knowingly or not) be required to store certain data for defined periods of time (up to 7 years) which may have an impact of archival capacity requirements
  - Budget – The planned budget to support the above considerations – rationalization of which may affect the business plan once the costs are known
- **Performance Requirements** – Capacity affects performance. Generally the first indicator that the capacity is not adequate will be a degradation of performance. In order to ascertain whether or not the level of performance warrants a change in capacity, the underlying requirements for performance must be understood.
- **MSP Supportability** – The MSP may require specific changes that affect capacity in order to efficiently manage the customer. As an example, many MSPs will require a centralized data storage model (all user data and profiles) which will reduce the capacity requirements of the workstation and simplify the data backup and recovery paradigm, but will contribute to the requirements for a centralized file store.

**Capacity Design**

The capacity design phase is focused on the development of a capacity plan. The capacity plan should include all planned capacity changes for the life of the managed services engagement (generally 12, 24, or 36 months) understanding that the longer the duration of the plan, the greater the level of uncertainty. Limitations to capacity planning will often include a lack of longer term business planning by the customer in which case the MSP will have to base a plan on resource consumption trends – all of which are subject to change based on better data. The simple goal is to be able to provide the customer with i) an accurate assessment on project plans to adjust capacity to suit the ongoing requirements and ii) to provide sufficient information to determine the costs associated to managing capacity in order to minimize the risks associated to a fixed fee managed services program.

Several key immediate deliverables fall out of the capacity plan:
- **IT architecture and design** – just as the MSP must consider the availability requirements when designing a supportable infrastructure, so too must they consider the immediate and mid-term capacity requirements.
- **Thresholds and alarms** – As part of the ongoing management of capacity, N-central will monitor the performance and resource levels of the underlying components. In order to make the monitoring useful and actionable the thresholds and alarms must be driven from the capacity plan.
- **Managed Services Program Cost** – The MSP must ensure that the cost of managing the capacity is considered in the ongoing cost of the program (if the planning and architecture is done properly, the management is typically not significant).

**Managing Capacity**

The management of capacity is a combination of monitoring the resource, performance and utilization levels of the underlying devices and analyzing that information on a periodic basis. The threshold and alarm information becomes a core component to changing the capacity data into relevant information. Additionally, the MSP should report on a periodical basis on the status of the capacity and capacity plans. The key report to support this activity is the executive summary report. The executive summary report is available in both N-central and N-compass however certain limitations present in the reporting infrastructure of N-central strongly suggest that N-compass is used for providing trended reports of any duration (longer than a week). Capacity information should be trended over months in order to develop an accurate growth trend.

As with all customer facing reports, the executive summary report should be delivered to the customer by an analyst. The report analysis is a key element to interpreting this report into information that affects the customer’s business – which is a significant component to the value of the managed services program.

**IT Service Continuity Management**

IT Service continuity management, sometimes known as disaster recovery, is the process of recovering from a ‘disaster’ in reasonable amount of time – a defined period of time that is considered to be acceptable to the business. Given the number of blackouts, hurricanes and other major disasters that many businesses experienced over the past few years, many business owners and CIOs (in larger organizations) are reexamining their disaster recovery strategies.

For the typical managed services customer a disaster may be something as minor as the loss of a key laptop all the way to a major disaster such as a fire or flood where the entire IT infrastructure is effectively destroyed.
Note: consider the implications of losing the business owners laptop, will business plans, financials etc and no backup.

Larger companies have other significant considerations as well - major U.S. regulations such as SOX, HIPAA and GLBA force corporate executives to develop business and IT continuity and disaster recovery strategies.

Most organizations do not have the resources to design and implement their own disaster recovery plan, which puts the organizations at the risk. To avoid these problems the MSP should offer a disaster recovery service aimed at protecting corporate assets in case of a disaster.

Ideally IT continuity management should be designed to support a larger business continuity plan. In practice many managed services customers (especially in the SMB) have never considered business continuity planning, and the MSP can’t wait until the customer develops one. As with many things a basic disaster recovery plan is better than no disaster recovery plan, so it falls to the MSP to educate the business owner on the critical assets that must be protected and help them build a plan that provides adequate protection for the business at an overall cost that the customer can manage.

Overall IT continuity management is an evolutionary process that must continue to adapt and change to meet the changing needs of the customer. As illustrated in Figure 9, the process is cyclical, being comprised of the following major phases:

- IT continuity planning
- Implementation
- Management
- Measurement

![Figure 9: IT service continuity process evolution](image)

After which time the cycle starts all over again with a complete review of the disaster recovery plan, incorporating lessons learned as well as accommodating new business requirements.
IT Continuity Planning

At a high level the objective of IT continuity planning is to understand how IT support the business operations and build a plan that makes sure the IT support of those operations is back up and running again in the right amount of time, where ‘right’ is defined as the appropriate balance of cost and recovery time.

To plan effectively, organizations need to assess their mission-critical business processes and associated applications before creating the full disaster recovery plan. In order to assess the impact of a disaster on the organization, the MSP should help the customer address the following questions:

- How much of the organization’s resources could be lost?
- What are organizational total costs?
- What efforts are required to rebuild?
- How my customers are affected, what is the impact on them?

As shown in Figure 10 IT continuity planning is comprised of five (5) major activities:

- Threat/Risk assessment
- Business impact analysis
- IT continuity strategy planning
- Data/systems backup planning
- Data/systems recovery planning

A threat/risk assessment is basically an inventory exercise – an inventory of the IT services within the business, as well as their relative priorities and an inventory of the potential threats. Threats to an organization might include fire, flood, terrorism, earthquake and tornado [non exhaustive]. The MSP must work with the customer to uncover all threats to each IT service.

A business impact analysis is designed to rate the impact to the business should a threat occur and to rate the likelihood of occurrence. It is a combination of the business impact and the likelihood that drives priority. From the business impact assessment two key elements emerge:
Recovery time objective (RTO) – The recovery time objective determines the desired span of time between failure and recovery. Every IT service requires an RTO. The RTO will be a key influencer in the architecture of the IT continuity strategy – the continuity strategy around a service with an RTO measured in minutes will be very different from that of a service where the RTO is measured in days.

Recovery point objective – Recovering a system generally has two main requirements: recovery the physical infrastructure, including networking, systems, operating systems and applications – all of which is relatively static; and recovering the system data, which may be highly dynamic. The recovery point objective asks the question ‘how much data loss is acceptable?’ The closer the answer gets to ‘none’ the more expensive the overall solution will be.

Once the recovery time objective and the recovery point objective are known, the MSP (in conjunction with the customer) are in a position to develop an IT continuity strategy for every IT service. Even low priority services require a plan for recovery. There are a number of common IT continuity strategies, including:

- Do nothing and pray for the best – Not an advisable approach. When customer’s think that this is appropriate, the MSP should advise them to try and live without the IT service for an extended period of time.
- Return to paper based process – This is an acceptable strategy for lower priority IT services – especially where the volume of work being done is relatively low (especially if the work will need to be redone once the IT systems are available). A key consideration for this approach is whether or not the paper-based approach is still available.
- Reciprocal agreement – A very viable strategy in the MSP model, where the MSP agrees to host the systems for the duration of the disaster, until primary systems can be recovered. (Please read the follow on Note below)
- Gradual recovery (cold standby) - A reasonable strategy for systems with a relatively long RTO (3 days +). A cold standby requires available space in an alternate network location, such as a collocation facility. Upon failure, systems are provisioned, built and data recovered.
- Intermediate recovery (warm standby) – A better strategy for systems that must be up and running within 48 hours. In a warm standby situation the systems are already provisioned at the alternate network location ready for the data to be recovered. This approach dramatically reduces the recovery time, but does increase the overall cost as the systems must be provisioned in advance and maintained in an identical state of readiness to the primary systems (i.e.: same level of service packs and updates to the systems they are intended to replace)
- Immediate recovery (hot standby) – A fail-over strategy where operations are immediately assumed by the standby system (at the alternate network location) upon failure provides near immediate recovery with virtually no human intervention. Ideal for absolutely critical IT systems where the relatively high implementation cost is acceptable.

Note: The MSP model lends itself nicely to the reciprocal IT continuity approach as several key requirements are already in place (or can be in place with relative ease) based on the type of relationship in place. The MSP, as a key influencer of IT purchases, can ensure that the physical systems are of a standardized type that the MSP is likely to have in the lab (or in inventory). Additionally most MSPs manage the static component of the software backup (O/S and applications) through the use of images – which are likely to be stored at the MSP location. This type of service adds tremendous value to the IT continuity component of a managed services engagement.

Having defined the overall IT continuity strategy for each service, the MSP begins the tactical planning component of defining the procedures and policies that protect the intellectual assets of the customer. There are two primary areas of concern for MSPs that should be considered separately:

- Operating system and applications (systems baseline) – The operating system and applications change very little (with the exception of service packs) and as such do not require a regular backup approach. A better approach is coordination with the change management to archive the systems baseline. Change management needs to test major changes to customer configurations prior to deployment. Implementing a process to ensure that images are produced when these major changes are introduced requires very little overhead – and satisfies the requirements of IT continuity management. **It’s not recommended to create a new archive for every minor change (such as an update or service pack) as long as the information exists in the change log that documents the changes that have occurred since the image (baseline) was taken. When the work associated to re-implementing the changes becomes significant, the MSP may choose to create a new baseline that includes all of the updated changes.
- Application data – Data is created through normal operations of the customer business. Whether that be transactional data within a database or updated/new documents, data is highly dynamic and represents a significant asset to the customer (consider the cost as being a function of the time required to create the data and the value it provides the customer). Backup strategies will be put in place that consider i) the frequency of data change ii) the priority of the data and iii) the total cost of the data backup strategy (including the MSP time to manage the backup strategy).
The other half of planning how to save the data is planning on how to get the data back into operation when required. This level of planning includes defining triggers for the IT continuity management process (we start when...), as well as defining responsibilities and owners and documenting the processes (and order) by which data is recovered remembering that different services (thus different data) has different recovery time objectives. The MSP should have much of this documentation already created (assuming that they are not working on their first customer) and as such the recovery planning is a matter of applying existing materials to a new customer.

Once the implementation (next step) is complete it is important to test the IT continuity plan because the last thing the MSP (or the customer) wants is to discover during an actual emergency that some key element was overlooked. Ideally a planned test will function exactly like a true disaster; the primary systems will offline and the disaster recovery processes will kick in. The main points are to measure the ability to achieve the recovery time and recovery point objectives. A post-test review will help to fine tune the plan.

**IT Continuity Implementation**

Once the plan is complete and approved the operational components must be implemented within the customer infrastructure. Key elements within the implementation include:

- Data backup – Tools, profiles and schedules need to be implemented and tested to ensure the veracity of the data backup (please see the MSP Management Tools Deployment Guide)
- System images – The MSP may not have system images for a new customer
- Customer training – All of the users must be trained on what they should do if the IT continuity plans kick in

**Manage the IT Continuity Plan**

The IT continuity management process requires very little in terms of ongoing attention – with the exception of customer awareness, disaster recovery testing and training to ensure a reasonable state of readiness the management activities are minimal. Unless of course disaster strikes, in which case management of the disaster recovery processes becomes the key initiative.

**Measurement and Improvement**

During planned tests as well as actual disaster scenarios, the MSP should take action to measure the efficiency and effectiveness of the IT continuity process. Additionally, post-disaster review meetings should occur with the MSP staff and representatives from the customer to understand where things went well, where things did not go well and understand how to improve the overall process. As with all managed services activities these lessons learned should serve to improve the overall process for the betterment of all of the MSPs customers.