The Problem with the ITIL Change Management Process

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

The Cost of Loose Change....

According to research from Gartner Group, “80 percent of unplanned downtime is caused by people and process issues”.

To explain further, we need to examine the following:

- Process Issues - the Change Management Process was bypassed or inadequately executed
- People Issues - Simply that the change was planned or implemented incorrectly

No Process = IT Anarchy

A formalized Change Management process is vital in order to maximize the effectiveness of any change while minimizing potential problems resulting from a configuration change being made.

Common sense quickly determines the need for some form of process. Imagine running your IT Service Delivery organization without any processes and no Servicedesk to keep records on Incidents logged, no Knowledgebase to avoid re-inventing the wheel for recurring problems, no Impact Analysis to avoid creating more problems during planned maintenance – the list goes on.

‘ITIL Best Practises’ identify Change Management as one of the key, central processes that should be understood and assimilated into an IT Service Delivery operation.

Change Management as a process is intended to ensure that when changes are made, they are first verified as being completely necessary and adding some value to the organization, and if so, that changes are then well planned, documented, and clearly communicated to ensure any potential negative impact from the change is understood and eliminated or minimized. The entire experience and knowledge of the enterprise is harnessed and greater efficiencies can be gained from ‘one visit’ fixes i.e. a number of required changes can all be delivered during one planned maintenance window.

A well maintained Configuration Management Database (CMDB) will often be used as a means of better understanding the ‘downstream’ effects of changes and/or their impact on a number of critical business services.

The elements of ‘verification’ and ‘communication’ have meant that Change Management systems that focus on the workflow and documentation have often naturally resided alongside or within the Servicedesk tool.

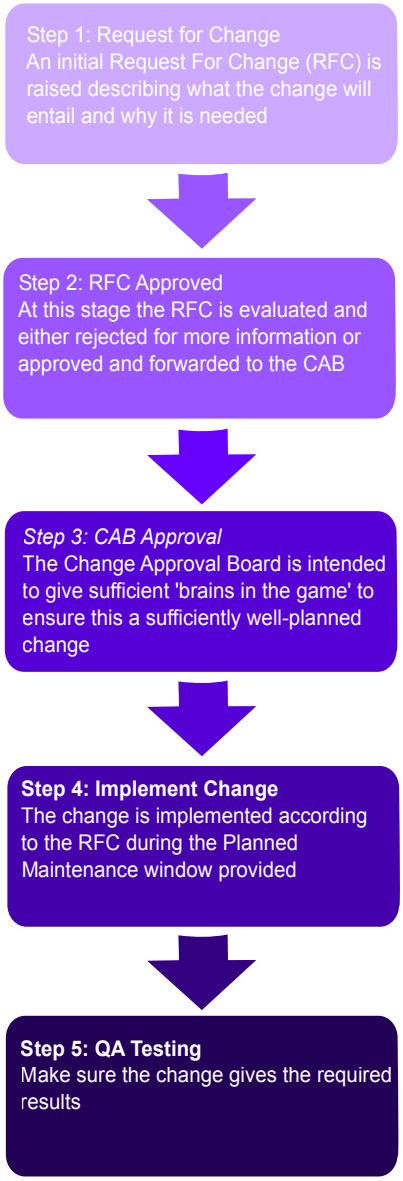


Figure 1 - A Typical Change Management Process

If it Ain't Broke...

The majority of changes to the IT infrastructure arise reactively in response to problems i.e. fixes. In addition, changes can be driven as proactive measures to improve service delivery, for instance, adding extra capacity to systems to improve performance or fault tolerance.

Whatever the drivers involved, changes are inevitable and in many organizations, hundreds of changes will be made each week, each and every one carrying the potential to create problems.

> *Research from IDC reports that "Operator error is the single largest source of outages, causing nearly 60 percent of overall infrastructure downtime".*

"Research from IDC reports that "Operator error is the single largest source of outages, causing nearly 60 percent of overall infrastructure downtime""

Furthermore, the problem is made more acute by every network device and server becoming more complex in configuration terms over the last few years.

For example, VLAN configuration used to be a premium feature on a network switch, but these days, it seems every device can switch, route, firewall, prioritize and shape traffic, before encrypting it into secure tunnels, not to mention handling voice and video, too.

> *EMA report that "98% of security breaches to virtual systems will be as a result of configuration error"*

"EMA report that "98% of security breaches to virtual systems will be as a result of configuration error""

Microsoft servers in particular present another level of challenge given that there are a wide range of configuration settings and attributes spread around the Operating System. Of course, servers are increasingly presented as virtualized entities which bring in a further factor of complexity to their configuration settings.

To Summarize the Issues Relating to Change Management

Changes are inevitable and therefore must be dealt with using proper planning and execution.

A formalized change process is therefore essential in order to fully assess, verify, approve, and test any changes made, with proper documentation and planning of what, how, where, and when changes will be made.

Any change carries a high potential to cause problems, even if it has been vetted through a rigorous Change Management Process first.

The Cost of Loose Change...

There are two key issues that arise in every organization we speak to, and both will always cause problems at regular intervals. In summary, these are in line with the Gartner statement we highlighted earlier – either the change management process is bypassed or not adhered to fully, or mistakes are made in making the change.

Would anyone in your IT Service Delivery team make any of the following statements?

'It's a small change so no need to run it through the Change Management Process'

Most organizations are either maturing in their adoption of a Change Management process, or just transitioning to a more formalized system. Many are using manual systems now but plan on using their Servicedesk or aligned workflow-application, whereas others consider themselves 'small enough' to not need what they consider to be overly bureaucratic processes.

Either way, it is widely accepted that there are different levels of changes which get handled in different ways according to their rating. Briefly and typically, 'big' changes go through the Change Management Process, whereas 'small' changes just get done.

The distinction between 'big' and 'small' is a judgement made by the individual based on unwritten, qualitative, grey definitions and herein lays one of the big problems.

'I implemented the planned change and took the opportunity to tidy up some other things – but that was Friday and I can't recall what else I changed now?'

As we have already discussed, any change – planned or unplanned - is capable of causing problems. With a Planned Change, there is a lifeline available in that the change was expected, planned, and documented and therefore rectification of any problem can take place immediately. With unplanned changes, we are right back in IT Anarchy – and if the individual that made the change has already gone home for the day, the rest of the team could be in for a long night...

A variation on the theme above is when a planned change is being made, and the engineer making the changes seizes the opportunity to make an additional 'quick' enhancement based on what they have seen.

'It was an emergency and there just wasn't time to document the changes made'

The Fire Fighting Change – no time to run through the change management process, we have got an emergency and need to work around it fast! This could be a Wide Area Network link failure where the backup link doesn't kick in, or traffic is not being routed properly through the backup path. In this instance, the change is made with best intentions at heart but unless the new configuration is backed up and a record made of the change then any potential side-effects introduced (for instance, when the primary link is restored but the network is slow), will need a lengthy investigation to eventually identify that all traffic is still being passed through the emergency backup path.

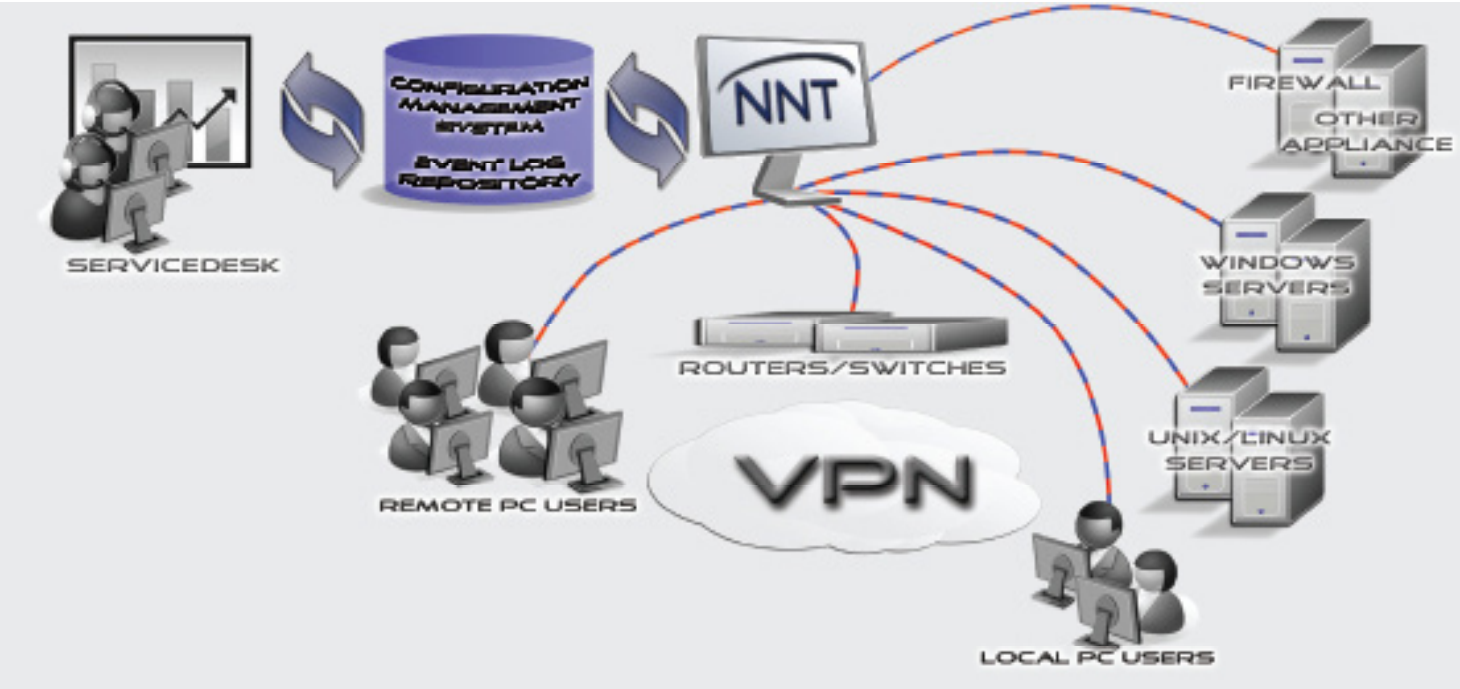
Automated Change and Configuration Management for the Enterprise

We have identified a number of flaws and weaknesses common to most organizations' implementation of the Change Management process. It is clear that we need an automated 'safety net' that will document and register all changes, regardless of whether the change is planned and/or authorized or not.

To be truly valuable and effective, any automated change monitoring system will need to be comprehensive – not just covering the network infrastructure components, but servers, and even user workstations, too.

Relatively speaking, network devices are straightforward – configuration settings are readily accessible through TFTP (Trivial File Transfer Protocol), SNMP or the device CLI (Command Line Interface), and are in text format.

Similarly, more advanced devices such as firewalls or appliances can be handled in the same way, using 'agentless' technology to extract and monitor configuration settings. Likewise, 'agentless' scripted interactions will be effective for Unix and Linux servers.



Automate Change and Configuration Management for the Enterprise

Microsoft OS servers have a wide range of configuration settings held in different formats and areas of the OS. Whilst performance metrics, such as CPU and Disk Usage can be gathered using SNMP, there are many more settings that need to be monitored to provide a configuration management safety net. Using an agent-based approach in the Windows environment is a big advantage and affords the opportunity to monitor

Application and Network Response Times - a local agent gives an ideal vantage point from which to measure 'user experience' of network and application service delivery

IIS Server and Web Site Settings - Monitoring configuration settings for the huge range of 3rd Party applications is too broad a brief, but vanilla applications should be covered

Registry Settings – the 'DNA' of the server, intended to be a central repository of OS, hardware and application settings

Services and Processes – changing service states, or adding new processes or services to a server or workstation may cause any number of problems

Installed Programs – in order to maintain a legal and cost-effective software portfolio it is necessary to control the usage and installation of Applications

Operating System – Service Packs and versions need to be controlled, as Windows Updates can easily introduce problems

User Accounts – potentially one of the most important settings to control, since adding or modifying a User Account could expose the server to further change

Vital Signs - Performance and capacity metrics

File Integrity – Secure Hash value, file sizes, file types, and folder structures

Not only is it crucial to track all the changes as detailed, but to do so in real-time, building a granular audit trail of changes so that when a problem does arise, the finite detail is available in a clear and easy to access manner.

There should be the flexibility to operate either as a safety-net, capturing all changes made and recording the details in a series of change records for reference when needed, or as a real-time alerting system whenever changes are detected. In addition, all changes and the results of those changes need to be recorded in order to meet any regulatory or governance requirements i.e. we did what we said we would do and therefore our systems remain in a 'known and compliant state'.

Lastly, an option to define a Configuration Policy is desirable, so that we not only track changes relative to a nodes' prior state, but also deviations from the preferred Policy.

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.