solid workflow options for integrating network change and configuration into IT operations more broadly, such as in support of lifecycle asset and capacity planning. HP is also looking to integrate network configuration into a broader change and configuration management system through ties with the HP OpenView System Configuration Manager. Finally, HP will be able to leverage the full multi-dimensionality of the NCCM value proposition through an integration with its CMDB initiative.

Priorities in Managing Change

There are clearly two perspectives on managing change: a process-driven approach and a technology-driven approach. Both are critical and both are coming together across the industry, as best practice initiatives such as ITIL are pushing for a more proactive and controlled approach to managing change, and as new technologies in the marketplace are providing greater visibility of infrastructure configurations, while enabling policy-based vehicles for access control and process automation.

One of the most significant trends on the process side is reflected in the IT Infrastructure Library’s (ITIL’s) notion of a Change Advisory Board (CAB). The CAB is typically made up of a mixture of professionals, often with executive representatives from the Network Operations Center (NOC), the data center and the service desk, as well as individuals tasked with security and compliance. An optimally organized CAB may typically meet once a week for about half an hour with capabilities for emergency reviews. Changes to critical infrastructure Configuration Items (CIs) are proactively assessed and reviewed, while the practice of “cowboy heroes” coming in to “save the day” is gradually eliminated. As one writer pointed out, the same cowboy who can save the day can just as easily miscalculate and make things orders of magnitude worse. The fact that more than 60% of problems in service performance come from configuration changes (in some cases 90%) and the fact that the great majority of those are caused by human error should help to underscore why 300%-400% ROI from such process initiatives isn’t exaggeration.

As this report will detail, good configuration management solutions can dramatically ease and enhance this cultural shift towards proactive control by providing accurate configuration awareness, accurate and well integrated audits, effective access control, and automated capabilities to identify and respond to problems.
Critical Drivers for Managing Change

There are a number of factors creating an increased demand for managing change more effectively. Some of the most salient are:

- **IT services and organizational missions are more and more intermixed** – IT’s impact on businesses is growing in importance. IT missions not only enhance productivity, they create new services, reach new markets, and integrate new partners into a company’s business model. In other words, the boundary lines between IT performance and business performance are becoming increasingly porous.

- **Increased operational efficiency** – To support the business effectively, IT must provide services with maximum efficiency. Change automation is a means to drive expenses down.

- **Geographic/(global) sprawl** – As an overall trend, workplaces, just like markets, are becoming increasingly decentralized. This ups the ante in how organizations accommodate more flexible and dynamic business models, with changing organizational dynamics.

- **More services, denser devices, greater frequency of change** – In parallel, businesses and government organizations are demanding a greater variety of IT services than in the past, including requirements for new technologies such as VoIP, Web Services and wireless. Largely as a result of this need, infrastructure devices have become orders of magnitude denser and more complex, while changes to the infrastructure through new application services, adds, moves and changes, patches and other updates are orders of magnitude more frequent.

- **Cascading failures in changing device configurations** – Given the frequency of change and increased infrastructure density, it’s no surprise that IT organizations are seeking new ways of working, especially since configuration problems often cause cascading failures across the infrastructure. In one IT environment EMA documented that eight out of ten changes to the network required other changes to be made, and 10% of the time, these resulted in catastrophic failures.

- **Security issues** – Security problems have become an even greater hazard, increasing the risks of poor configurations and upping the costs of poor Mean-Time-To-Repair (MTTR).

- **Compliance issues** – While compliance issues have brought configuration management into the limelight, they do place an overhead “tax” on IT that can be disruptive to day-to-day management without effective automation in generating audits and reports.

- **IT best practices and IT governance** – While these initiatives, such as the CAB described above, are part of the cure for the problem, they also demand time, effective toolsets, cultural changes and organizational maturity.

- **Financial accountability** – Since IT services are so directly intertwined with business performance, it isn’t surprising that businesses are looking for IT to show accountability not only in quality of service, but in cost effectiveness, value and relevance. Managing change effectively becomes fundamental in optimizing infrastructure for service performance, while providing clear advantages in support of IT initiatives such as data center consolidation, or WAN rightsizing and operational and infrastructure costs.

**IT Priorities**

As shown in Figure 1, configuration management tops the list of IT concerns, followed by visibility – or seeing both planned and unplanned changes, visualizing the entire IT configuration, and accurately assessing the impact of changes.

Interestingly enough, network configuration stands out as the single most important area of concern in managing configuration changes. For instance, two years ago network provisioning topped the list for areas of greatest configuration activity followed by security and server provisioning. Current data shows that network configuration management similarly tops the list for priorities in populating Configuration Management Databases (CMDBs), followed by systems configuration, software release information, topology and inventory.
A word or two should be said about CMDBs, since they are helping to transform the way both vendors and IT adopters are approaching change management. A “CMDB” is a concept defined by ITIL as a consistent and dynamic resource for critical infrastructure configuration, topology, asset, and other information regarding infrastructure hardware and software as they all map to IT services, as well as to IT operational owners and customers. As such, the CMDB goes far beyond most conventional definitions of “configuration management” from the perspective of documentation. (ITIL separates the active changes made to the infrastructure from its discipline of configuration management, grouping this activity under the category of “release management.”) The dramatic rise in interest in CMDB deployments is in some environments outstripping ITIL itself, as it reflects the need to integrate and reconcile different management investments into a more consistent and coherent strategic resource.

The central role of configuration management in ITIL is not simply a coincidence. It underscores how critical configuration information can be in supporting not only managing configuration changes, but in providing a consistent and dynamic context to support virtually all management disciplines – from incident, problem and availability management, to security and capacity planning, among others.

The Evolution of the NCCM Market

Although there were precedents for the multi-vendor network change and configuration management marketplace as early as the late 1990s, the NCCM marketplace has evolved largely over the last four years. The market has been fueled by the growing frequency of making changes, the need to provide a consistent and reliable auditing mechanism for change management across brands, the need to dramatically reduce the time-consuming processes associated with recovery from configuration change errors, and growing frustration with the inefficiencies and limitations of existing element management systems. NCCM vendors have also accelerated their acceptance through linkages to best practices and compliance.

As multiple vendors entered the market, IT adopters began to look for the following design requirements:

- Ease of deployment, use, and maintenance.
- Multi-vendor support, which was interestingly enough a requirement even in environments that were virtually single brand or homogeneous. These IT adopters felt that having a process as strategic as change and configuration control confined to a single hardware choice was unacceptable.
- Easy extensibility to new devices and models.
- Audits to show the difference between what's changed and what's not.
- Alerts on non-policy-compliant changes.
- Alerts on security-related threats.
- High quality and flexible reports including reports both scheduled and on request. It was also important that NCCM reports support a number of roles including service desk, administrator and executive, as well as the traditional network engineer user.
- Authorized access controls in order to integrate network configuration and change management with requirements for compliance, IT governance, security and best practice initiatives. This includes the ability to edit and manage Access Control Lists (ACLs) and audits that show who changed what device configuration and when the change was done.
- Scalability, as most early adopters planned initially small implementations that would stage incrementally to large, complex network deployments.
- Active SW distribution (ITIL’s “Release Management”) that includes the ability to store many multiple versions of past configurations for disaster recovery and restore to “golden” state.
- The ability to perform some level of inventory and discovery.
- Support for integrations with network management and other solutions such as help desk, asset management, security, etc.
• Integration with element managers such as CiscoWorks.
• Support for event and workflow integration.
• Initial cost and incremental pricing models to support flexible adoption strategies.

**HP OpenView Network Configuration Manager**

On June 8, 2006, HP announced HP OpenView Network Configuration Manager to provide configuration, audit, compliance, and change management control for the networked infrastructure. The new configuration management capabilities were the result of a well-planned investment in network configuration management technology through an OEM agreement with Voyence, Inc., based in Richardson, Texas. Voyence is one of a handful of network configuration management vendors that have helped to create the NCCM market. Voyence also has the single most balanced market acceptance across enterprise, government and service provider verticals.

More specifically, HP’s Network Configuration Manager supports configuration and release management requirements for wireless LAN switches, wireless access points, routers, ATM/WAN switches, LAN switches, content switches, firewalls, VPN concentrators, load balancers, DSL routers, multi-service switches, traffic shapers, VoIP switches, storage directors and integrated access devices. The Network Configuration Manager manages more than 1,000 device models from 35 different hardware vendors, which is one of the broadest device support capabilities in the marketplace. As such, it complements the capabilities provided by HP OpenView System Configuration Manager based on Radia technology from Novadigm.

Network Configuration Manager leverages robust object-based modeling technologies in support of policy-based automation, and is a natural fit with Radia-based technologies, as well as with HP’s long term architectural commitment to model-based automation. It is worth noting that Voyence had introduced CMDB support earlier in 2006 in order to ensure that its systems could actively participate in federated CMDB environments. These design considerations should help to further HP requirements in the intermediate-term for a more systemic approach to change, configuration, compliance, asset management and service assurance, as will be explained in more detail below.

**Core Functionality and Near-term Integration**

HP OpenView Network Configuration Manager ships with an integration solution for Network Node Manager. Through this integration, network managers seeking to relate shifts in network performance and availability with recent changes made to the infrastructure will have a cohesive set of navigational options to do so. HP is also investing in correlation capabilities to tie configuration changes with service delivery issues so that the linkages become more quickly and readily visible. In most IT environments, when coupled with process initiatives, this should result in dramatic reductions in service performance issues. For example, in some environments configuration-related errors can be reduced from 90% of those impacting service performance to as low as 10% or less.

As a vehicle for managing change, HP OpenView Network Configuration Manager delivers on all the functional requirements listed in the “Evolution of the NCCM Market” section. Some of the highlights of what HP’s solution can additionally offer from both a benefits and functions perspective include the following:

• **Intelligent automation and operational efficiencies** – EMA has seen time reductions of 500% and better when network configuration management has been used to implement planned changes, or respond to unplanned events.
• **Design new networks based on existing designs** – Network Configuration Manager can capture and reuse existing configurations associated by policy with specific network environments. Replication of these can then be effectively automated, with dramatic gains in operational efficiency and drastic reductions in human error. In support of this automation, Network Configuration Manager provides auditing capabilities to ensure that planned configuration changes conform to policy before they are activated.
• **Diagnostic and resolution of security issues** – Security problems are often configuration-related and network configuration tools can shorten the time to respond to security threats by 1000% or more, while helping to minimize the likelihood of serious security attacks.
• **Support for ITIL best practices and process initiatives** – ITIL has rightly identified effective configuration visibility and process control as at the heart of successful IT Service Management. Network Configuration Manager provides audits, policy-based workflows, and access control capabilities that support ITIL requirements.
• **Flexibility of access control and access audits** – Network Configuration Manager has built-in capabilities for managing access control based on policy as per specific device, customer environment, individual, organization...
and role. EMA expects these to quickly be enhanced through HP's broader capabilities in identity management and IT governance.

- **Flexibility of compliance support for HP’s compliance initiatives** – Accurate audits for network configuration changes and reporting are required for effective compliance management.

### Longer-term Integration Potential

HP is well aware that network change and configuration management is not a siloed or niche discipline, but one that is more of a enabler for supporting a broad array of requirements and disciplines. Some of the areas to watch in HP's future announcements are:

- **Service Desk integration with workflow for process integration** – This should be achieved in the second half of 2006. It will provide broad capabilities for integrating network configuration process with processes in other disciplines from asset management, to service assurance, to security and compliance.

- **Integration with HP OpenView System Configuration Manager for integrated change and configuration management across the broader infrastructure (e.g. applications and servers).** This will provide more cohesive support for optimizing operational processes and provide superior consistency for assuring services, provisioning services and adapting the infrastructure to changing business requirements.

- **Integration to support HP’s CMDB initiative** – HP will also be introducing CMDB integration in 2007. Such integration will enable a more holistic approach to managing change across network and systems environments, as well as making network configuration information available to a other management applications in other disciplines based on policy and access rights. Once again, these will range across areas such as asset management, service level management and service planning, incident and problem management, security and compliance, and of course configuration, change and release management.
EMA Assessment

EMA is very positive about HP’s announced HP OpenView Network Configuration Manager. Probably the most major reservation is that it wasn’t done sooner. But even so, HP has stolen the high ground from all of its traditional Enterprise Systems Management (ESM) competitors in this space, while moving towards a unique breadth and depth of integration that most of its newer competitors – in network management and configuration management – will likely be unable to imitate.

To optimize its advantage, HP will need to make clear, fast advances in its integration strategies in workflow and Active CMDB. If HP can do this, and EMA believes it will, it should be able to offer its customers a truly strategic change and configuration control system across the full infrastructure, while enjoying a clear competitive edge in this increasingly structural and process-centric market.
About Enterprise Management Associates, Inc.

Enterprise Management Associates is an advisory and research firm providing market insight to solution providers and technology guidance to Fortune 1000 companies. The EMA team is composed of industry respected analysts who deliver strategic awareness about computing and communications infrastructure. Coupling this team of experts with an ever-expanding knowledge repository gives EMA clients an unparalleled advantage against their competition. The firm has published hundreds of articles and books on technology management topics and is frequently requested to share their observations at management forums worldwide.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

©2006 Enterprise Management Associates, Inc. All Rights Reserved.

Corporate Headquarters:
2585 Central Avenue, Suite 100
Boulder, CO 80301

Phone: +1 303.543.9500
Fax: +1 303.543.7687