Essential NCPI Management Requirements for Next Generation Data Centers

By Ted Ives

White Paper #14

Legendary Reliability®

Executive Summary

The management of physical infrastructure in data centers can no longer be considered independently of the IT management architecture. In order to manage rapid change and achieve demanded levels of availability while controlling Total Cost of Ownership, IT managers can no longer afford to rely on the primitive, customized management solutions of the past. These solutions are no longer effective and must be replaced by systems based on, and integrated with, open IT management standards. With this in mind, this paper describes the requirements for management of next-generation Network-Critical Physical Infrastructure from the perspective of the ITIL framework.

Introduction

The key to managing Network-Critical Physical Infrastructure (NCPI) is to employ the same strategies used in the management of servers, storage, switches, and printers. The core issues of maintaining system availability and managing problems and change are similar, although each device may have specific problems based on its unique characteristics. Essential categories of management for NCPI include Incident Management, Change Management, Capacity Management, and Availability Management. Implementing the suggested strategies will contribute to successful application of the ITIL framework to all aspects of data center operations.

In this paper, a systematic approach of identifying and classifying user problems provides insight regarding the nature and characteristics of NCPI management in next generation mission critical installations.

NCPI

Network-Critical Physical Infrastructure

NCPI is the foundation upon which IT and telecommunication networks reside.

NCPI includes:

- Power
- Cooling
- Racks and physical structure
- Cabling
- Physical security and fire protection
- Management systems
- Services

For more about NCPI see APC White Paper #117, "Network-Critical Physical Infrastructure: Optimizing Business Value"

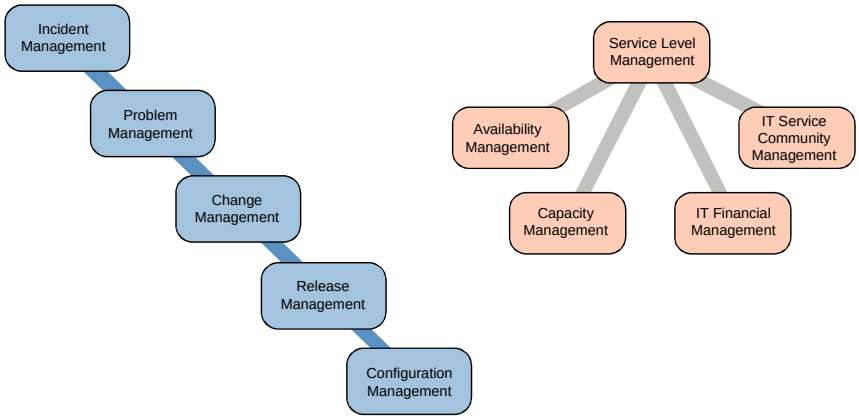
What is Management?

Any discussion of management issues must first define what is meant by "management". The topic of "management" is a broad one, which is easy to get lost in without a logical framework for discussing it. The Information Technology Infrastructure Library (ITIL) is one such framework that many customers and equipment suppliers have found helpful in understanding the various aspects of management.

ITIL is a set of guidebooks defining models for planning, delivery, and management of IT services, created by the British Standards Institute and owned by the UK Office of Government Commerce. ITIL is not a standard but a framework whose purpose is to provide IT organizations with tools, techniques, and best practices that help them align their IT services with their business objectives. IT organizations typically select and implement the pieces that are most relevant to solving their business problems. The categories and guidelines defined by ITIL can be extremely helpful in determining and achieving IT service management objectives, and many IT vendors such as HP, IBM, and Microsoft have used ITIL as a model for their operations framework.

ITIL's "Service Support" and "Service Delivery" models each include several processes, and although they are often depicted in introductory presentations as having a simple organization with just a few connections (as in **Figure 1**), when one reads the ITIL documentation in detail, it becomes clear that all the processes are interconnected via a myriad of process flows.

Figure 1 – ITIL processes



ITIL "Service Support" processes (focused on end-users)

ITIL "Service Delivery" processes (focused on business owners)

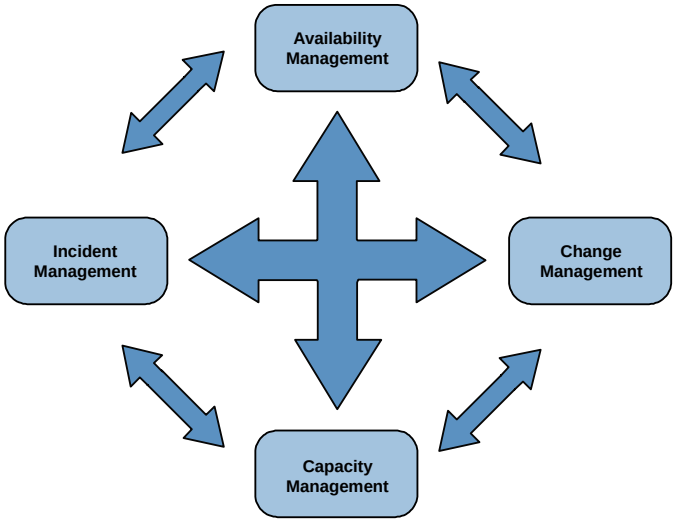
Although the ITIL processes are all related in one way or another, it is not necessary to analyze the entire spectrum of processes and flows – Identifying which ones are critical and relevant to managing NCPI is a helpful aid in achieving success in the "Zero Layer" of the data center hierarchy. ITIL is a wide-encompassing framework, and a complete explanation of it is out of the scope of this paper. The reader is encouraged to visit www.itil.co.uk for further information on ITIL itself.

This paper will identify the most critical management processes as defined by ITIL for management of NCPI, and outline key problems and requirements for effective NCPI management in each area.

Key ITIL processes for managing Network-Critical Physical Infrastructure

Although most ITIL methodologies contain useful suggestions and describe various connected processes, the most important ones to consider when managing NCPI are outlined in **Figure 2**. The remainder of this white paper addresses the key management challenges that each of these processes presents.

Figure 2 – Key processes for management of Network-Critical Physical Infrastructure



NCPI Management Challenges in Mission Critical Installations

Using the ITIL process model, the challenges and underlying problems in the NCPI layer are presented in four charts corresponding to the four key ITIL management processes of **Figure 2**.

Incident Management

This process is concerned with returning to the normal service level (as defined in a negotiated Service Level Agreement or SLA between the IT group and internal business process owner) as soon as possible, with the smallest possible impact on the business activity of the organization and user.

NCPI, like any other IT equipment, should be monitored, with events fed into an Incident Management process, either via an NCPI Incident Management system or a general-purpose Incident Management tool such as a Network Management or Building Management System.

Incident Management Challenges		
Challenge	**Underlying Problems**	**Management System Requirements**
Identify where the problem is physically located and what the logical impact of the problem is	NCPI includes diverse yet interconnected components – when an event occurs it can be difficult to quickly ascertain where the problem lies (for instance, when there is a problem along the power path somewhere between the main panel and the network switch itself in the rack).	System level view that indicates the relationships between interconnected components and identifies the impact of individual component problems.
Identify owner of the problem resolution	Responsibility for NCPI availability is often shared, potentially leading to redundant and conflicting efforts to resolve incidents. Different people are responsible for different locations at different times of the day / week. In critical systems such as NCPI systems there is frequently an escalation path of responsibility.	System that provides ability to set and assign user roles for notification, incident and resolution ownership purposes. Management tool that notifies the responsible authority at any given time, and if the situation is not corrected, escalates notification as appropriate.
Prioritize urgency level of incident	Incidents that aren't prioritized are dealt with in an inefficient manner. This may lead to downtime if higher priority events are not addressed. Additionally, some events (such as leaving a UPS in bypass after maintenance or having a Computer Room Air Conditioner filter that needs changing) may not be urgent, but they should have high priority.	A management tool that alerts the user to the impact, urgency, and priority of individual events that threaten system availability.
Take proper corrective actions to return the system to normal service levels	NCPI includes components ranging from power to cooling to network cabling – when an event occurs it can be difficult for one person to have all the expertise necessary to troubleshoot all issues.	A system that provides recommended actions and guidance to return the system to the normal condition.

Availability Management

Availability Management is concerned with systematically identifying availability and reliability requirements against actual performance, and when necessary, introducing improvements to allow the organization to achieve and sustain optimum quality IT services at a justifiable cost.

Once NCPI requirements have been established, service levels must be monitored, with particular care given to understanding the potential downtime that can result from individual components *failing* and their impact on the entire system.

Availability Management Challenges		
Challenge	**Underlying problems**	**Management System Requirements**
Report on availability metrics	Creating and tracking availability metrics can be difficult and time consuming. These are necessary in order to track achievement against service levels agreed upon between IT and the internal business customer.	A tool that provides uptime and downtime reporting, downtime summaries (NCPI versus non-NCPI), causes of downtime, system redundancy, drill down to individual incidents, incident timestamp and duration, and time to recovery.
Receive advanced warning of impending failures	Easily correctable problems with NCPI often go unnoticed until a failure occurs.	A system that provides alerting and global thresholds for UPS runtime, power distribution unit load by phase, battery health, and rack temperature and humidity. Information that is presented in an easy to understand manner that does not require training or expert knowledge.
Manage and minimize impact of planned downtime	Planned downtime *is a necessary thing* in many data centers, but tools that do not take into account planned downtime can have two negative effects: 1. Spurious alerts leading to incorrect actions by personnel. 2. Maintenance modes left uncorrected after maintenance is complete (such as a UPS left in bypass, or a cooling unit offline).	A system that allows scheduled maintenance windows, both suppressing alerts during the window and alerting the user to any maintenance conditions left uncorrected after the window has closed.
Continuously improve availability of data center infrastructure	ITIL recommends making continuous improvements to availability plans and infrastructure, but often expertise to attain these higher levels of availability is lacking.	Management tools that provide a risk assessment summary to identify potential areas for improvement, such as insufficient runtime, options for adding cooling redundancy, moving load to a different phase, and moving IT equipment to different rack.

Capacity Management

This process is concerned with providing the required IT resources at the right time, at the right cost, aligned with the current and future requirements of the internal customer. Power, cooling, rack space, and cabling are all IT resources that require capacity management. Product architectures that allow incremental purchases of these resources on short time frames are

preferable to legacy architectures that require specifying, engineering, purchasing, and installation over yearlong timeframes, particularly with regard to Total Cost of Ownership (TCO) considerations. Any NCPI management system needs to address the following challenges in this area:

Capacity Management Challenges		
Challenge	**Underlying Problems**	**Management System Requirements**
Monitor and record changes in data center equipment and infrastructure	As additional equipment is added to the data center over time, existing power and cooling capacity may be inadvertently exceeded resulting in downtime. NCPI systems require attention as UPS batteries age over time. Rate of battery aging is dependant on factors such as temperature and usage. In addition to high temperature levels, fast rates of change (even if the absolute levels are within operating limits) can permanently damage IT equipment.	A system that monitors current draw for each branch circuit or rack and alerts the appropriate person to potential overload situations. A system that reports on any UPS systems that have exceeded minimum runtime or maximum load thresholds to ensure that SLAs can be met. A system that monitors temperature and humidity at the rack level and alert the appropriate person to potentially damaging temperature and humidity levels. A system that monitors temperature rate of change to ensure IT equipment is not damaged by rapid changes in environmental conditions.
Provide NCPI capacity when and where it is needed to support business needs	IT refreshes are dynamic in nature and difficult to predict. NCPI capacity requirements often go unnoticed until it is too late.	A management tool that provides trending analysis and threshold violation information on UPS load, runtime, power distribution, cooling, rack space utilization, and patch panel port availability to ensure adequate advance notice and information necessary for procurement and deployment of additional capacity.
Optimize physical layout of existing and new equipment	IT equipment changes sometimes result in sub-optimized data center space and increased capital and operating expense.	A management tool that recommends optimal placement and layout of new IT equipment, to meet power, rack space, cooling, and cabling needs.
Scale data center infrastructure incrementally	As infrastructure is added to the data center, it can be difficult to reconfigure tools to monitor the new objects; licensing schemes that focus on charging per “data point” can be cost prohibitive.	Tools that leverage existing IT infrastructure investment and monitor additional new NCPI devices in an economical, simple and quick way.

Change Management

This process is concerned with methods and procedures for making changes to infrastructure with the lowest possible impact on service quality, and is increasingly critical for optimizing business agility. Maximizing the ratio of planned to unplanned work in a data center requires formalized change management processes for all aspects of operation. Changes such as relocating a server, rewiring a patch panel, or moving equipment from a warmer area of a data center to a cooler area are examples of changes requiring preparation, planning, simulation, and an audit trail. Any NCPI management system needs to address the following challenges in this area:

Change Management Challenges		
Challenge	**Underlying Problems**	**Management System Requirements**
Execute adds, moves and changes of IT equipment without impacting availability	When equipment is moved: ▪ Circuit breakers are accidentally tripped or UPS systems are accidentally overloaded. ▪ Appropriate power plug types are not available. ▪ Insufficient data ports are available on patch panels. ▪ Insufficient cooling is available resulting in hot spots. ▪ Heat may not be removed adequately in individual areas (although the average thermal capacity for overall room may be adequate). ▪ Insufficient rack space is available.	A management tool that provides planning to ensure the NCPI system will meet the needs of IT equipment changes and makes recommendations on optimized layout utilizing both existing and new NCPI. Tool that recommends workflow for planning, executing and tracking changes.
Implement firmware changes in individual NCPI components	Firmware upgrades that are performed during normal operating hours can lead to downtime and or reduce SLA performance.	A system that allows scheduling for any firmware upgrades to occur during off-hours.
Maintain all NCPI components at supported revisions and combinations of firmware	Firmware upgrades provide additional functionality as well as bug fixes and are essential to overall system health. However, ever-increasing volume of responsibilities are being placed upon network administrators, making it extremely difficult to maintain awareness of proper firmware revision levels, particularly when an interconnected system requires multiple components with different firmware that communicates within the architecture.	A system that notifies the administrator whenever new bug fixes or feature enhancements to firmware are available, and provides mass remote upgrade capabilities.
Maintain spares at compatible firmware revision levels	When spares are swapped into a modular architecture they may not be at a supported firmware revision / combination, causing downtime.	An NCPI management solution that ensures that spares match production equipment, so when a spare module is swapped in, no problems occur.

Where to Start

APC's extensive field experience has shown that, although most organizations implement aspects of all the processes outlined here, most will develop their management strategy in the following order:

1. Implement an **Incident** Management system
2. Set and measure **Availability** targets
3. Monitor and plan for long term changes in **Capacity**
4. Then…get **Change** Management processes in place

Organizations typically focus on fully implementing each management process for three to six months before moving on to the next.

Conclusion

As the foundation layer supporting the information technology, applications and processes that ITIL strives to improve, NCPI plays an important role in attaining agreed upon service requirements. A full-featured NCPI management solution that is based on and integrated with open IT systems is essential in order to manage rapid change and achieve demanded levels of availability while controlling TCO.

When designing, planning, deploying, and operating any NCPI solution, particular care should be given to ensure that the availability, incident, capacity, and change management processes are properly addressed. Only by careful attention and successful implementation of these processes can the IT manager meet the challenges of maximizing the availability and efficiency of their IT infrastructure and enable a more agile data center capable of responding dynamically to changes in business requirements.

References

APC White Paper #100, "Management Strategies for Network-Critical Physical Infrastructure"

"Service Support", "Service Delivery", "ICT Infrastructure Management"
UK Office of Government Commerce, 2002

About the Author:

Ted Ives is Director of Business Development with APC in West Kingston, RI, and is responsible for Partnership and Strategy Development.