Enterprise Management System White Paper

FCAPS, TMN & ITIL

Three Key Ingredients to Effective IT Management

Written by:

Jeff Parker
Managing Partner
OpenWater Solutions, LLC
jeff@owsol.com

May 6, 2005

www.openwatersolutions.com

Executive Summary

Maintaining the health of an enterprise's infrastructure is a fundamental requirement of business today. Employees rely on IT services to perform their jobs. Customers rely on IT services to perform business. In both situations, the clients mandate availability and performance of key systems and applications. When problems do arise IT must be able to quickly identify and resolve these problems. Mean time to repair (MTTR) needs to be as short of duration as possible. Continuous, non-stop availability and reliability of the IT infrastructure is a must for any enterprise.

Key to providing a robust infrastructure to clients and employees is the strategic management of all IT services and elements. Strategic infrastructure management allows an enterprise to proactively manage its IT service availability, utilization, and growth. Proactive management allows less downtime, rapid problem resolution, lower costs, and higher reliability of services.

Because of the diversity and complexity of typical IT infrastructures, the design and implementation of an effective Enterprise Management System (EMS) is crucial. A complete implementation for the EMS will consider integration with current tools, staffing, IT process, reporting, and other key factors.

IT Management – Where to Start?

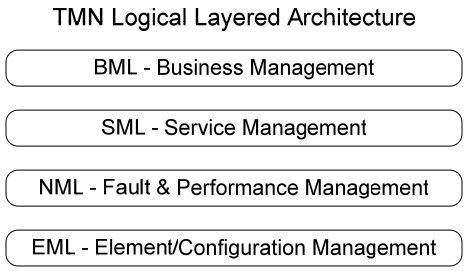
The need to manage organizations IT Infrastructure is obvious, right? Most organizations do a good job of managing their critical IT Assets – don't they? You'd be surprised. You'd be hard pressed to find a CIO publicly state that managing their IT Infrastructure is a secondary concern or a low priority. Why is it then, that most organizations do such a poor job of managing their IT Infrastructures? The answer is simple: lack of discipline, diligence, planning and organization.

Unfortunately many organizations get so consistently bogged down in putting out fires on a daily basis that they never have time to sufficiently address IT Management. Years of experience in IT has shown that IT Management is typically always a Top 10 priority at most companies. How can it be that most companies have still not adequately addressed this important topic? There are a number of reasons. Probably the most important is that while IT Management is always a Top 10 priority; it never quite makes it to Top 5 – relegating it to stagnation as an unfunded, unassigned, and ultimately ignored initiative. Another reason is the IT industry's poor track records in delivering IT Management solutions that actually work. After 36 months 70% of IT Management solutions are no longer being used. A big part of this problem is vendors making proclamations that their products can live up to. The second part of the equation is the technology buyers who believe these vendor claims even though history shows that most infrastructure management tools are either never implemented correctly or quickly become 'shelfware'.

TMN Model

So where does that leave us? Where do we go from here? A good place to start is the basics. Standards do exist for building IT Management solutions. One of the first was developed by the International Telecommunication Union (ITU-T; formerly CCITT). ITU-T was created in March of 1993, replacing the former International Telegraph and Telephone Consultative Committee (CCITT) whose origins go back to 1865. The public and the private sectors cooperate within ITU-T for the development of standards that benefit telecommunication users worldwide. ITU-T's mission is to ensure an efficient and on-time production of high quality standards (Recommendations) covering all fields of telecommunications. Back in May of 1996 the ITU-T introduced recommendation M.3010, which delivered the concept of TMN or Telecommunications Management Network. Recommendation M.3010 was developed as a framework for service providers to manage their service delivery networks. M.3010 consisted of four management architectures at different levels of abstraction: functional, physical, informational and logical layered. It is at the Logical Layered Architecture were applicability to corporate

IT Management really begins to unfold. The Logical level introduced the concept of four layers of abstraction, which is represented as follows:

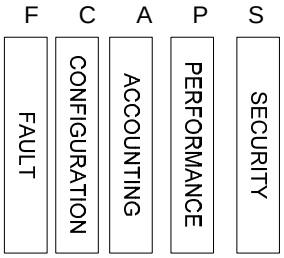


This model provides a crisp correlation between IT Assets and their performance with the ability of the business to function as required. Or to put it another way, alignment between IT and the Business – something most IT Departments are striving to accomplish.

FCAPS Model

This is a good start, but more is needed. Thankfully the ITU-T again came out with a recommendation. This one was introduced in April of 1997 as Recommendation M.3400. M.3400 introduced us to the concept of FCAPS.

In addition to the TMN layering structure, the ITU–T also splits the general management functionality offered by management systems into the five key areas of fault, configuration, accounting, performance, and security (FCAPS). This categorization is a functional one and does not describe the business-related role of a management system within the telecommunications network. The idea of FCAPS stems directly from the ITU–T recommendations and describes the five different types of information handled by management systems. Portions of each of the FCAPS functionality will be performed at different layers of the TMN architecture. As an example, fault management at the EML (Element Management Layer) is detailed logging of each discrete alarm or event. The EML then filters the alarms and forwards them to an NML (Network Management Layer) that performs alarm correlation across multiple nodes and technologies to perform root-cause analysis.



Although the ITU-T initially developed the concept of FCAPS to assist in managing telecommunications networks it was really the International Standards Organization who applied the concept to data networks. ISO delivered the FCAPS Framework called the Open Systems Interconnect (OSI) Network Management Model as the basis for most network management implementations. The OSI model specifies five functional areas, which fall under the network management umbrella. These functional areas are, **F**ault Management, **C**onfiguration Management, **A**ccounting (or Asset/Inventory) Management, **P**erformance Management, and **S**ecurity Management. This model is commonly referred to as the **FCAPS** model. Each of these functional areas is described below.

Fault Management
Recognizing problem situations is only the first step in Fault Management. To have an effective Fault Management system also requires the ability to isolate problems to the source, provide notification to the appropriate person(s), and track problems through resolution via a trouble ticketing system.

Configuration Management
Configuration management addresses the essential area of managing device configurations. It is one of the most important ways that a network manager can control the health of the network. By keeping regularly scheduled configuration backups and having carefully controlled implementation and change procedures this can be achieved. Another aspect to consider with configuration management is the ability to track changes that are made to the device configurations.

Accounting Management
Concerns usage statistics and allocation of costs associated with billing for time and services provided by devices and/or resources.

Performance Management
To manage a network effectively requires the ability to track short and long-term network and system statistics. The collected data, which may include utilization, errors, response time, and availability, can be valuable tools when identifying network trends and considering capacity planning.

Security Management
Security Management concerns access rights, data privacy, and auditing security violations. In most implementations, this usually entails controlling access to network hardware components.

A subset of the FCAPS functionality is listed below.

F	C	A	P	S
Fault detection	Resource initialization	Track service / resource usage	Utilization & error rates	Selective resource access
Fault correction	Network provisioning	Cost for services	Consistent performance level	Enable NE functions
Fault isolation	Auto-discovery	Accounting limit	Performance data collection	Access logs
Network recovery	Backup and restore	Combine costs for multiple resources	Performance report generation	Security alarm / event reporting
Alarm handling	Resource shut down	Set quotas for usage	Performance data analysis	Data privacy
Alarm filtering	Change management	Audits	Problem reporting	User access rights checking
Alarm generation	Pre-provisioning	Fraud reporting	Capacity planning	Take care of security breaches & attempts
Clear correlation	Inventory/asset management	Support for different modes of accounting	Performance data & statistics collection	Security audit trail log
Diagnostic test	Copy configuration		Maintaining & examining historical logs	Security related information distributions
Error logging	Remote configuration			
Error handling	Job initiation, tracking & execution			
Error statistics	Automated software distribution			

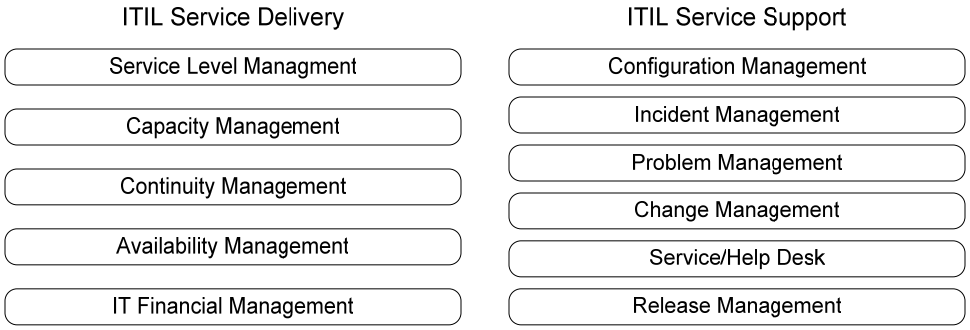
ITIL

ITIL (Information Technology Infrastructure Library) is a set of best practices standards for Information Technology (IT) service management. The United Kingdom's Central Computer and Telecommunications Agency (CCTA) created ITIL in response to the growing dependence on Information Technology to meet business needs and goals. ITIL provides businesses with a customizable framework of best practices to achieve quality service and overcome difficulties associated with the growth of IT systems.

ITIL is organized into sets of texts which are defined by related functions: service support, service delivery, managerial, software support, computer operations, security management, and environmental. In addition to texts, ITIL services and products include training, qualifications, software tools, and user groups such as the IT Service Management Forum (itSMF).

By the mid 1990's ITIL had become the world-wide de facto standard in service management. ITIL is currently one of the fastest growing business optimization initiatives sweeping across North America. ITIL processes are being adopted by organizations both big and small due to its ability to improve business processes. ITIL focuses on best practices, and as such can be adapted and adopted in different ways according to each individual organizations needs. So what is it?

While owned by the CCTA since the mid-1980s, ITIL is currently maintained and developed by the Office of Government Commerce. The Service Management section of ITIL is made up of eleven different disciplines, split into two sections, Service Support and Service Delivery:



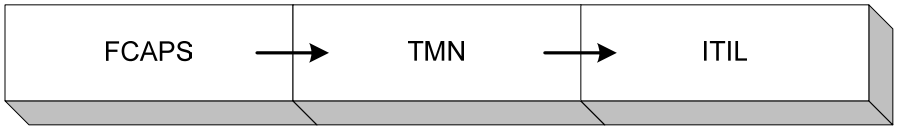
One of the primary factors leading to such rapid growth and adoption of ITI are the benefits being reported by users. Many of the common themes being reported are cost reductions, operational efficiency, and better alignment of IT and the Business.

Summary

A simple review of the three standards shows that TMN, FCAPS and ITIL all overlap in terms of concepts that they address. It is true that they do speak to some of the same concepts. They do so at completely different levels of abstraction. FCAPS is primarily focused on the concept of technology management. TMN focuses on service management. TMN presents technology at a level that the business can understand; not just your network administrator. ITIL on the other hand, is all about the process for how to run an efficient IT organization. ITIL focuses on process and workflow.

Now that we have explained three different standards the question remains – where to start? The topic of where to start is one of heated debate. Many consulting organizations are pushing widespread adoption of ITIL within organizations. This is good for the adopting organization and great for the consulting company. It should mean years of consulting revenue for the consulting company in training, workshop facilitation, project management, process mapping, etc.

A good place to start is to consider the data needed to make the support decisions that your organization requires. A model that is based this premise looks as follows:



The above model presents a good approach for adoption of IT Management. It is also pragmatic in that is should allow companies to realize that their IT Management Roadmap is not complete after they purchase their first fault management tool. IT Excellence is an ongoing effort that requires commitment and discipline. Understanding the journey that will be embarked upon allows for realistic expectation setting. Disclaimer: Every organization is different and its needs may dictate a different approach.

This isn't to say that ITIL adoption should not occur or should be delayed. There just may be another approach. There is an old axiom that states "you cannot manage what you don't measure and you cannot measure what you don't collect." An organizational wide ITIL initiative for a large company may take years of effort. Does that mean that it's acceptable not to manage the IT assets in the meantime? Of course not! The above model is meant to address this fact.

An FCAPS initiative will at least give your organization the necessary data collection points to:

- Understand when a problem occurs
- Identify the performance characteristics of key IT components
- Properly engineer IT architectures based on capacity data available
- Understand when configuration changes are occurring in order to react appropriately
- Identify security breaches as they occur

Once FCAPS is soundly under way you'll soon hear IT Leadership asking for service views or dashboards showing more complex technology views. For example, you may be asked to present a dashboard showing the status of the organizations eCommerce website or perhaps a view of the Human Resource Management System. This is where TMN comes into play. It provides mechanisms to tie together the discrete data collection points that FCAPS offers and present them in service centric dashboards or views.

This level of sophistication is typically much more important to IT Leadership. Most CIO's do not care if you can ping across their network 100% of the time or if the Dallas, Texas router is operational. They care whether or not the organizations key applications are up and running and meeting defined service level expectations; thereby allowing the organization to perform the functions necessary to run the business.

Once an organization is collecting the required data and presenting that data in a meaningful fashion the savvy IT Leader will understand the need to optimize the processes and workflow to allow IT to better support the business. This is not to say that this shouldn't be considered during the FCAPS and TMN initiatives. It needs to be. The point to be made is that IT needs to deliver services that are up and performing to the organization every day. Waiting two years for the business to map out all of the processes prior to implementing IT Management solutions will only make for a painful two year stretch.

Conclusion

FCAPS starts with a technology centric view. TMN layers on top a service oriented view. ITIL then adds on process optimization and efficiency to the equation. For organizations seeking operational excellence a combination of all three standards is the key to success. FCAPS has proven to be a logical and low risk starting point. Follow up FCAPS by integrating the TMN concepts of Business & Service Level Management. Lastly, put a plan in place to optimize the organization by deploying ITIL best practices.

References

1. From FCAPS to ITIL: An Optimized Migration, February 21, 2005, by Suparno Biswas
2. International Telecommunications Union website for overview info of ITU-T